计算数学丛书

数论变换

蒋增荣

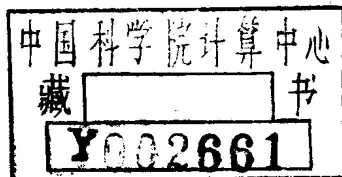


计算数学丛书

数 论 变 换

蒋 增 荣

上海科学技术出版社



内 容 提 要

七十年代以来出现的数论变换是一种以数论为基础的计算循环卷积的方法。它是在以正整数 M 为模的整数环（域）Z_M 上定义的线性正交变换，所用的计算方法是数论中的同余运算。它在 Z_M 上具有循环卷积特性，基本函数又是由整数的方幂构成。本书从数学的角度介绍数论变换的原理、性质、快速算法，Mersenne 数变换，Fermat 数变换，伪 Fermat 数变换，复数数论变换，二维数论变换和减少字长的方法，数论变换的应用等。

本书可供高等学校计算数学专业的学生及研究生参考，也可供高等学校数学系和计算机科学系的师生以及计算数学工作者参考。

计算数学丛书

数　论　变　换

蒋　增　荣

上海科学技术出版社出版

（上海瑞金二路 450 号）

新华书店上海发行所发行　上海市印刷三厂印刷

开本 787×1092 1/32　印张 6.25　字数 137,000

1980 年 8 月第 1 版　1980 年 8 月第 1 次印刷

印数 1－12,000

书号：13119·841　　定价：(科四) 0.60 元

出版说明

《计算数学丛书》是为了适应计算数学和计算机科学的发展，配合高等院校计算数学教学的需要而组织的一套参考读物。读者对象主要是高等院校数学系和计算机科学系的学生、研究生，亦可供高等院校数学系和计算机科学系的教师以及工矿企业、科研单位从事计算工作的技术人员参考。

本丛书向读者介绍近代计算方法的一些主要进展及其适用范围和实用效果。每种书集中介绍一个专题，针对本专题的近代发展作综合性的介绍，内容简明扼要，重点突出，有分析，有评价，力图使读者对该专题的动向和发展趋势得到一个完整的了解。

本丛书已拟定的选题计有：《线性代数与多项式的快速算法》、《数论变换》、《数值有理逼近》、《矩阵特征值问题》、《Sobolev 空间引论》、《计算组合数学》、《样条与逼近》、《有限条形法》、《广义逆矩阵及其计算方法》、《非线性方程迭代解法》、《奇异摄动》、《Walsh 函数及其应用》、《多项式最佳逼近》、《坏条件常微分方程数值解》、《最优控制问题的计算方法》、《误差分析》、《最小二乘问题的数值解法》、《快速傅里叶变换》、《板壳问题非协调方法》、《外推法》、《并行算法》、《Padé 逼近》、《Monte Carlo 方法》、《差分格式理论》、《高维偏微分方程数值解》、《初值问题差分方法》等二十余种，将于一九八〇年初起陆续出版。

前言

近年来，数字式信号处理在无线电电子学领域如遥感、自动控制等方面，甚至在无线电电子学以外的地震、石油勘探、医学技术等部门都获得了广泛的应用．采用线性变换的方法是数学上分析线性非时变系统的一种手段．其中最常用的就是离散傅里叶变换 (Discrete Fourier Transform，简写为 DFT)．1965 年 Cooley 和 Tukey 提出了离散傅里叶变换的快速算法 (Fast Fourier Transform，简记为 FFT)，大大节省了计算工作量，从而缩短了处理时间．因此，七十年代初期，许多部门中都已使用了 FFT.

但是，在数字信号序列的长度 N 很大的情况下，利用 FFT，计算量仍然很大．用 FFT 做一个 N 点的复信号变换，大约需要 $N\log_2 N$ 次复数乘法及 $N\log_2 N$ 次复数加法．利用 FFT 的循环卷积特性计算 N 点的循环卷积，需要三次变换及 N 次复乘，同时还存在舍入误差，从而不能得到高精度的卷积．此外，由于 DFT 的基本函数是三角函数，所以必需预先贮存基本函数.

能不能在保持循环卷积特性的前提下，采用比三角函数更为简单的基本函数呢？正如本书 **2** 中所证明的，在复数域内，具有循环卷积特性的唯一变换是 DFT．因此，在复数域内，不存在既具有循环卷积特性、基本函数又比三角函数更简单的线性正交变换．但是，事物是发展的，最近提出的一种以数论为基础的计算循环卷积的方法，已引起了人们的重视，这

种方法就叫做数论变换.

数论变换是在以正整数 M 为模的整数环(域) Z_M 上定义的线性正交变换,所用的运算法则是数论中的同余运算,它在 Z_M 上既具有循环卷积特性,基本函数又是由整数的方幂构成.特别是 Fermat 数变换(Fermat Number Transform,简记为 FNT),其基本函数由 2 的方幂构成,变换长度 $N=2^m$.因此,在二进制计算机上,FNT 根本不用乘法,仅为移位操作,且具有 FFT 类型的快速算法.又由于是模运算,所以不存在舍入误差,从而能得到高精度的卷积.此外,也不需要基本函数的贮存.但是,FNT 也有缺点.主要是它没有物理意义,在信号处理中不能运用中间过程;其次是估计误差有困难;再次就是字长比较受限制,不够灵活,并且所需字长与变换点数之间存在着严格的关系.尽管如此,数论变换在发展中将会不断地完善起来.

本书从数学的角度较系统地介绍了数论变换的原理,性质,快速算法,Mersenne 数变换,Fermat 数变换,伪 Fermat 数变换,复数数论变换,二维数论变换和减少字长的方法,最后介绍了它在其它方面的应用以及它所应用的代码.其中的定理和公式,都严格地做了证明.为便于不熟悉数论基本知识的读者阅读,在第三章还介绍了一点必要的数论基本知识.

本书在写作过程中,始终得到孙本旺教授、汪浩教授等许多同志的热心支持和帮助,特表示感谢.

由于作者水平所限,书中难免有错误,恳切希望同志们批评指正.

作　者　1979.3.

目　　录

— 1 —

卷积与循环卷积

设两个长为 N 的序列 x_n 和 $h_n(n=0, 1, \cdots, N-1)$，其卷积是指*

$$y_n=\sum_{k=0}^{N-1} x_k h_{n-k}=\sum_{k=0}^{N-1} x_{n-k} h_k \quad (n=0, 1, \cdots, N-1). \quad (1)$$

其中假定 $x_n=h_n=0(n<0)$. 这种卷积在用电子计算机进行信息处理时是经常用到的. (1)式的矩阵表示是

---

* 通常在数字滤波等应用中，将遇到两个长度不同的序列 $x_n(n=0, 1, \cdots, M_1-1)$，$h_n(n=0, 1, \cdots, M_2-1)$，其卷积

$$y_n=\sum_{k=0}^{M_1-1} x_k h_{n-k}=\sum_{k=0}^{M_2-1} x_{n-k} h_k$$

$$(n=0, 1, \cdots, M_1+M_2-2;\ x_n=h_n=0,\ n<0).$$

但这种卷积可以通过补零变成长度相同(长度均为 M_1+M_2-2) 的卷积(1)，输出序列 y_n 的长度亦为 M_1+M_2-2. 例如，$x_n(n=0, 1)$，$h_n(n=0, 1, 2, 3)$，其卷积 y_n 的长度应为 4，即

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix}=\begin{bmatrix} h_0 & 0 \\ h_1 & h_0 \\ h_2 & h_1 \\ h_3 & h_2 \end{bmatrix}\begin{bmatrix} x_0 \\ x_1 \end{bmatrix}. \quad (a)$$

在所给序列 x_n 和 h_n 的后面补零而成为长度为 4 的序列 $(x_0, x_1, 0, 0)$，(h_0, h_1, h_2, h_3)，作它们的如下卷积

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix}=\begin{bmatrix} h_0 & & & \\ h_1 & h_0 & & 0 \\ h_2 & h_1 & h_0 & \\ h_3 & h_2 & h_1 & h_0 \end{bmatrix}\begin{bmatrix} x_0 \\ x_1 \\ 0 \\ 0 \end{bmatrix}. \quad (b)$$

由计算知，(a)式和(b)式所得结果相同.

由于上述原因，只需研究如正文(1)式那样序列长度相同、卷积序列长度亦相同的卷积.

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_{N-1} \end{bmatrix} = \begin{bmatrix} h_0 & & & & \\ h_1 & h_0 & & 0 & \\ h_2 & h_1 & h_0 & & \\ \vdots & \vdots & \vdots & & \\ h_{N-1} & h_{N-2} & h_{N-3} & \cdots & h_0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{N-1} \end{bmatrix}. \tag{1'}$$

通常用列矢量来表示序列 x_n 和 $y_n(n=0, 1, \cdots, N-1)$. 比如要求下列两序列的卷积:

$$(x) = \begin{bmatrix} 1 \\ 2 \\ 0 \\ -2 \\ 1 \end{bmatrix}, \qquad (h) = \begin{bmatrix} 1 \\ -2 \\ 1 \\ 0 \\ 1 \end{bmatrix},$$

按照(1)式或(1′)式, 我们有

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} 1 & & & & \\ -2 & 1 & & 0 & \\ 1 & -2 & 1 & & \\ 0 & 1 & -2 & 1 & \\ 1 & 0 & 1 & -2 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 0 \\ -2 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ -3 \\ 0 \\ 6 \end{bmatrix}.$$

直接计算(1)式, 大约需要 N^2 次乘法和 N^2 次加法, 当 N 很大时, 其计算量是超量的, 实际上难以完成且很费时间. 因此, 寻求快速算法以节省时间就是一件有意义的工作.

通常, 通过循环卷积来计算(1). 所谓两个序列 $x_n(n=0, 1, \cdots, N-1)$ 和 $h_n(n=0, 1, \cdots, N-1)$ 的循环卷积是指:

$$y_n = \sum_{k=0}^{N-1} x_k h_{\langle n-k \rangle_N} = \sum_{k=0}^{N-1} x_{\langle n-k \rangle_N} h_k$$
$$(n=0, 1, \cdots, N-1). \tag{2}$$

即

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_{N-1} \end{bmatrix} = \begin{bmatrix} h_0 & h_{N-1} & h_{N-2} & \cdots & h_1 \\ h_1 & h_0 & h_{N-1} & \cdots & h_2 \\ h_2 & h_1 & h_0 & \cdots & h_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ h_{N-1} & h_{N-2} & h_{N-3} & \cdots & h_0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{N-1} \end{bmatrix}. \tag{2'}$$

(2)式中的符号 $\langle k\rangle_N$ 表示整数 k 模 N 的最小非负剩余，也就是整数 k 被正整数 N 除所余的非负整数，例如

$$\langle 7\rangle_4=3, \qquad \langle -7\rangle_4=1.$$

从卷积与循环卷积的定义(式(1)和式(2))可知，它们是不同的. 比如上例中两个序列的循环卷积就是:

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & -2 \\ -2 & 1 & 1 & 0 & 1 \\ 1 & -2 & 1 & 1 & 0 \\ 0 & 1 & -2 & 1 & 1 \\ 1 & 0 & 1 & -2 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 0 \\ -2 \\ 1 \end{bmatrix} = \begin{bmatrix} -1 \\ 1 \\ -5 \\ 1 \\ 6 \end{bmatrix}.$$

下面的引理说明如何用循环卷积来计算卷积.

引理 1 两个长为 N 的序列 x_n 和 h_n，其卷积(1)可通过如下的两个长为 $2N$ 的序列 $\hat{x}_n$ $(n=0, 1, \cdots, 2N-1)$ 和 $\hat{h}_n$ $(n=0, 1, \cdots, 2N-1)$ 的循环卷积来计算.

设

$$\hat{x}_n=\begin{cases} x_n, & n=0, 1, \cdots, N-1, \\ 0, & \text{其它}; \end{cases} \tag{3}$$

$$\hat{h}_n=\begin{cases} h_n, & n=0, 1, \cdots, N-1, \\ 0, & \text{其它}; \end{cases} \tag{4}$$

$\hat{x}_n$ 和 $\hat{h}_n$ 的循环卷积记为 $\hat{y}_n$，即

$$\hat{y}_n = \sum_{k=0}^{2N-1} \hat{x}_k \hat{h}_{\langle n-k\rangle_{2N}} \quad (n=0, 1, \cdots, 2N-1),$$

则

$$y_n = \hat{y}_n \quad (n=0, 1, \cdots, N-1). \tag{5}$$

证明 由 $\hat{x}_n$ 的定义(3)知, 当 $n=0, 1, \cdots, N-1$ 时, 有

$$\hat{y}_n = \sum_{k=0}^{2N-1} \hat{x}_k \hat{h}_{\langle n-k\rangle_{2N}} = \sum_{k=0}^{N-1} x_k \hat{h}_{\langle n-k\rangle_{2N}}.$$

当 $n, k=0, 1, \cdots, N-1$ 时, 有

$$-(N-1) \leqslant n-k \leqslant N-1.$$

由定义(4)知,

$$\hat{h}_{\langle n-k\rangle_{2N}} = \begin{cases} h_{n-k}, & 0 \leqslant n-k \leqslant N-1, \\ 0, & -(N-1) \leqslant n-k < 0; \end{cases}$$

故

$$\hat{y}_n = \sum_{\substack{k=0 \\ 0 \leqslant n-k \leqslant N-1}}^{N-1} x_k h_{n-k}.$$

由假设, 当 $n<0$ 时, $h_n=0$, 故

$$\hat{y}_n = \sum_{k=0}^{N-1} x_k h_{n-k} = y_n. \qquad \text{证毕.}$$

读者如果用矩阵形式写出序列 $\hat{x}_n$ 和 $\hat{h}_n$ 的循环卷积 $\hat{y}_n$ ($n=0, 1, \cdots, 2N-1$), 则可明显的看出 $\hat{y}_n$ 的前面 N 个值恰是 x_n 和 h_n 的卷积 y_n($n=0, 1, \cdots, N-1$)的值.

在实际应用中, 还可能遇到一种有别于(1)式的卷积和(2)式的循环卷积, 称为恒定对角卷积(Constant Diagonal Convolution):

$$y_n = \sum_{k=0}^{N-1} x_k h_{n-k} \quad (n=0, 1, \cdots, N-1). \tag{6}$$

式中下标出现负值时, 不再如(1)式那样有 $h_n=0$, 也不如(2)式那样是周期的($h_n=h_{N+n}$). (6)式的矩阵形式是

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_{N-1} \end{bmatrix} = \begin{bmatrix} h_0 & h_{-1} & h_{-2} & \cdots & h_{-(N-1)} \\ h_1 & h_0 & h_{-1} & \cdots & h_{-(N-2)} \\ h_2 & h_1 & h_0 & \cdots & h_{-(N-3)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ h_{N-1} & h_{N-2} & h_{N-3} & \cdots & h_0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{N-1} \end{bmatrix}. \tag{7}$$

卷积(1)和循环卷积(2)都是这种卷积的特殊情况. 式(6)可看作两个序列 $(x_0, x_1, x_2, \cdots, x_{N-1})$ 和 $(h_{-(N-1)}, h_{-(N-2)}, h_{-(N-3)}, \cdots, h_0, \cdots, h_{N-1})$ 之间的一种卷积.

引理 2 设两个序列 x_n $(n=0, 1, \cdots, N-1)$ 和 h_n $(n=-N+1, -N+2, \cdots, 0, \cdots, N-1)$,其恒定对角卷积(6)可通过如下的两个长为 $2N$ 的序列 $\hat{x}_n$ 和 $\hat{h}_n$ 的循环卷积来计算.

设

$$\hat{x}_n = \begin{cases} x_n, & n=0, 1, \cdots, N-1, \\ 0, & \text{其它}; \end{cases} \tag{8}$$

$$\hat{h}_n = \begin{cases} 0, & n=0, \\ h_{-N+n}, & n=1, 2, \cdots, 2N-1; \end{cases} \tag{9}$$

$\hat{x}_n$ 和 $\hat{h}_n$ 的循环卷积记为 $\hat{y}_n$, 即

$$\hat{y}_n = \sum_{k=0}^{2N-1} \hat{x}_k \hat{h}_{\langle n-k \rangle_{2N}} \quad (n=0, 1, \cdots, 2N-1),$$

则

$$\hat{y}_{n+N} = y_n \quad (n=0, 1, \cdots, N-1). \tag{10}$$

证明 当 $n=0, 1, \cdots, N-1$ 时, 由(8)式知,

$$\hat{y}_{n+N} = \sum_{k=0}^{2N-1} \hat{x}_k \hat{h}_{\langle n+N-k \rangle_{2N}} = \sum_{k=0}^{N-1} x_k \hat{h}_{\langle n+N-k \rangle_{2N}}.$$

由于当 $n, k=0, 1, \cdots, N-1$ 时, 有

$$1 \leqslant n+N-k \leqslant 2N-1,$$

故由(9)式知, $\hat{h}_{\langle n+N-k \rangle_{2N}} = \hat{h}_{n+N-k} = h_{n-k}$.

于是 $$\hat{y}_{n+N}=\sum_{k=0}^{N-1}x_k h_{n-k}=y_n.$$ 证毕.

这个引理中的 $\hat{x}_n$ 和 $\hat{h}_n(n=0,\ 1,\ \cdots,\ 2N-1)$ 是由 x_n 和 h_n 通过补零和适当移位形成的. 读者仍可用循环卷积的矩阵形式(式(2′)), 来表示 $\hat{x}_n$ 和 $\hat{y}_n$ 的循环卷积 $\hat{y}_n(n=0,\ 1,\ \cdots,\ 2N-1)$, 利用矩阵的分块相乘法, 不难看出 $\hat{y}_n$ 的后面 N 个值就是 x_n 和 h_n 的恒定对角卷积 $y_n(n=0,\ 1,\cdots,\ N-1)$ 的值.

引理 1 和引理 2 分别将(1)式和(6)式化作循环卷积. 循环卷积可用变换法计算. 一般常用的变换为离散傅里叶变换(DFT).

DFT 的定义如下: 设序列 $x_n(n=0,\ 1,\ \cdots,\ N-1)$, 变换

$$X_k=\sum_{n=0}^{N-1}x_n W_N^{nk}\quad(k=0,\ 1,\ \cdots,\ N-1)\tag{11}$$

称为 DFT, 其逆变换(IDFT)为

$$x_n=\frac{1}{N}\sum_{k=0}^{N-1}X_k W_N^{-nk}\quad(n=0,\ 1,\ \cdots,\ N-1),\tag{12}$$

其中 $W_N=e^{-j\frac{2\pi}{N}}$.

利用复数域上 N 阶单位根的性质

$$\frac{1}{N}\sum_{n=0}^{N-1}W_N^{pn}=\begin{cases}1, & p\equiv 0 \pmod N,\\ 0, & p\not\equiv 0 \pmod N,\end{cases}\tag{13}$$

不难证明(11)和(12)确是一对互逆变换. 事实上, 将(12)式代入(11)式, 得

$$\sum_{n=0}^{N-1}\left(\frac{1}{N}\sum_{m=0}^{N-1}X_m W_N^{-nm}\right)W_N^{nk}$$

$$=\frac{1}{N}\sum_{m=0}^{N-1}X_m\left(\sum_{n=0}^{N-1}W_N^{n(k-m)}\right)\quad(k=0,\ 1,\ \cdots,\ N-1),$$

利用(13)式, 可知上式右端为 X_k.

(11)式和(12)式可写作如下矩阵形式:

$$(X)=T_N(x) \tag{11'}$$

$$(x)=T_N^{-1}(X) \tag{12'}$$

其中，$(x)=\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{N-1} \end{bmatrix}$，$(X)=\begin{bmatrix} X_0 \\ X_1 \\ X_2 \\ \vdots \\ X_{N-1} \end{bmatrix}$，

$$T_N=\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & W_N & W_N^2 & \cdots & W_N^{N-1} \\ 1 & W_N^2 & W_N^4 & \cdots & W_N^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & W_N^{N-1} & W_N^{2(N-1)} & \cdots & W_N^{(N-1)^2} \end{bmatrix},$$

$$T_N^{-1}=\frac{1}{N}\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & W_N^{-1} & \cdots & W_N^{-(N-1)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & W_N^{-(N-1)} & \cdots & W_N^{-(N-1)^2} \end{bmatrix}.$$

DFT 最重要的性质是循环卷积特性，即两个序列 x_n 和 h_n 的 DFT 的乘积等于其循环卷积 y_n 的 DFT：

$$Y_k=X_k\cdot H_k \quad (k=0,\ 1,\ \cdots,\ N-1),$$

或

$$\text{DFT}\{y_n\}=\text{DFT}\{x_n\}\cdot\text{DFT}\{h_n\}. \tag{14}$$

这是由于

$$Y_k=\sum_{n=0}^{N-1}y_nW_N^{nk}=\sum_{n=0}^{N-1}\left[\sum_{m=0}^{N-1}x_mh_{\langle n-m\rangle_N}\right]W_N^{nk}$$

$$=\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}x_mh_{\langle n-m\rangle_N}W_N^{nk},$$

记 $n-m=l$，则

$$Y_k=\sum_{m=0}^{N-1}x_m\left[\sum_{l=-m}^{N-1-m}h_{\langle l\rangle_N}W_N^{k(l+m)}\right];$$

而 $$\sum_{l=-m}^{N-m-1} h_{\langle l\rangle_N} W_N^{k(l+m)} = \sum_{l=-m}^{-1} h_{\langle l\rangle_N} W_N^{k(l+m)} + \sum_{l=0}^{N-m-1} h_{\langle l\rangle_N} W_N^{k(l+m)},$$

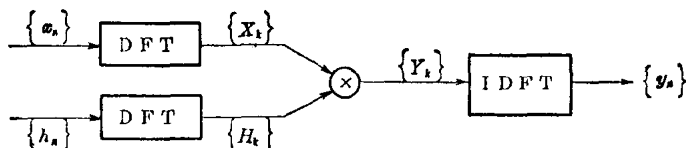
由于 $$h_{\langle l+N\rangle_N} = h_{\langle l\rangle_N}, \quad W_N^{k(l+m+N)} = W_N^{k(l+m)},$$

故 $$\sum_{l=-m}^{-1} h_{\langle l\rangle_N} W_N^{k(l+m)} = \sum_{l=N-m}^{N-1} h_l W_N^{k(l+m)};$$

所以 $$\sum_{l=-m}^{N-m-1} h_{\langle l\rangle_N} W_N^{k(l+m)} = \sum_{l=0}^{N-1} h_l W_N^{k(l+m)}.$$

于是 $$Y_k = \sum_{m=0}^{N-1} x_m \left[\sum_{l=0}^{N-1} h_l W_N^{k(l+m)} \right] = \sum_{m=0}^{N-1} x_m W_N^{mk} \cdot \sum_{l=0}^{N-1} h_l W_N^{lk}$$
$$= X_k \cdot H_k.$$

利用 DFT 的循环卷积特性可以计算两个序列 x_n 和 $h_n(n=0,\ 1,\ \cdots,\ N-1)$ 的循环卷积 y_n，这只要分别计算 x_n 和 h_n 的 DFT，即 X_k，H_k，将它们相乘就得到 y_n 的 DFT，即 $Y_k = X_k \cdot H_k\ (k=0,\ 1,\ \cdots,\ N-1)$，最后将 Y_k 进行反变换(IDFT)，就得到 y_n. 示意图如下：



由上可知，利用 DFT 的循环卷积特性计算长为 N 的序列的循环卷积，需要两次正变换，一次逆变换和 N 次乘法. 一次变换需要 N^2 次乘法，所以共需要 $3N^2+N$ 次乘法. 当 N 较大时，计算量很大，比不用变换法而直接计算循环卷积的计算量大得多. 但是如果 N 是高度复合数，特别当 $N=2^m$(m 为自然数)时，用快速傅里叶变换(FFT)进行计算，计算量大

为减少．一个 N 点的变换用 FFT 计算约需 $N\log_2 N$ 次乘法，降低了两个数量级．如果 $\{h_n\}$ 的变换预先计算好，那么用 FFT 实现 N 点的循环卷积只需 $2N\log_2 N+N$ 次乘法．正是由于 FFT 的出现，DFT 才成为实用的方法．

以数论为基础的计算循环卷积的方法，在国内外已引起了重视，这种方法叫做数论变换(NTT)．特别引人注目的是 NTT 中有一种 Fermat 数变换(FNT)，这种变换只需加法(减法)及移位操作而不用乘法，从而提高了运算速度，这一点已为在通用计算机上的运算结果所证实．对于实现长度不超过 256 的序列的循环卷积，FNT 比 FFT 缩短了时间达三至五倍．下表列出了 R. C. Agarwal 与 C. S. Burrus 在 IBM 370/155 计算机上实现不同长度序列的循环卷积时，FFT 与 FNT 所需时间的比较：

表 1　实现长度为 N 的实序列的循环卷积计时

N	FFT(ms)	FNT 或 RT(ms)	N	FFT(ms)	FNT 或 RT(ms)
32	16	3.3	256	123	80.0(*)
64	31	7.4	512	245	166.0(*)
128	60	16.6	1024	530	340.0(*)
256	123	40.0	2048	1260	720.0(*)

其中，RT 为 FNT 的一种快速算法；(*)是用的二维 RT．

FNT 还消除了 FFT 带来的舍入误差，故能得到高精度的卷积，并且也不需要基函数的存贮，从而节省了存贮器．但是，FNT 也有缺点，主要是它没有明显的物理意义；序列 $\{x_n\}$ 的变换 $\{X_k\}$ 不再是频谱，因此中间过程不能如 DFT 那样用来测速或测频，同时估计误差有困难；再就是字长很受限制，不够灵活．但随着数论变换研究的深入及其算法的普及，数论变换将会不断地完善起来．

—2—

具有循环卷积特性的变换结构

考虑一线性非奇异变换 T，其元素记为 $t_{k,m}(k, m=0, 1, \cdots, N-1)$*:

$$T=\begin{bmatrix} t_{0,0} & t_{0,1} & t_{0,2} & \cdots & t_{0,N-1} \\ t_{1,0} & t_{1,1} & t_{1,2} & \cdots & t_{1,N-1} \\ t_{2,0} & t_{2,1} & t_{2,2} & \cdots & t_{2,N-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ t_{N-1,0} & t_{N-1,1} & t_{N-1,2} & \cdots & t_{N-1,N-1} \end{bmatrix}. \quad (1)$$

记序列 x_n 和 h_n 的变换各为 X_k, H_k, x_n 和 h_n 的循环卷积 y_n 的变换为 Y_k, 即

$$\begin{aligned} (X) &= T(x), \\ (H) &= T(h), \\ (Y) &= T(y). \end{aligned} \quad (2)$$

定义 如果变换 T 具有如下性质

$$Y_k = X_k \cdot H_k \quad (k=0, 1, \cdots, N-1), \quad (3)$$

则称 T 为具有循环卷积特性的变换.

定理 1 变换 T 具有循环卷积特性的充要条件是

$$t_{k,m} = \alpha^{km} \quad (k, m=0, 1, \cdots, N-1),$$

其中 α 为 N 阶单位根. 也就是说, T 必须且只须具有形状:

---

* 如果 k, m 在范围 0, 1, …, $N-1$ 之外，则作如下周期延拓:

$$t_{k+N,m} = t_{k,m}, \qquad t_{k,m+N} = t_{k,m}.$$

$$T=\begin{bmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{N-1}\\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(N-1)}\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ 1 & \alpha^{N-1} & \alpha^{2(N-1)} & \cdots & \alpha^{(N-1)^2}\end{bmatrix}. \tag{4}$$

证明 先证充分性. 设 T 具有(4)的形状. 由于

$$X_k=\sum_{n=0}^{N-1}x_n\alpha^{nk},$$

$$H_k=\sum_{n=0}^{N-1}h_n\alpha^{nk},$$

$$Y_k=\sum_{n=0}^{N-1}y_n\alpha^{nk},$$

故
$$Y_k=\sum_{n=0}^{N-1}y_n\alpha^{nk}=\sum_{n=0}^{N-1}\left[\sum_{m=0}^{N-1}x_mh_{\langle n-m\rangle_N}\right]\alpha^{nk}$$
$$=\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}x_mh_{\langle n-m\rangle_N}\alpha^{nk}.$$

记 $n-m=l$, 则

$$Y_k=\sum_{m=0}^{N-1}x_m\left[\sum_{l=-m}^{N-m-1}h_{\langle l\rangle_N}\alpha^{k(m+l)}\right]=\sum_{m=0}^{N-1}\sum_{l=0}^{N-1}x_mh_l\alpha^{km+kl}$$
$$=\sum_{m=0}^{N-1}x_m\alpha^{km}\cdot\sum_{l=0}^{N-1}h_l\alpha^{kl}=X_k\cdot H_k.$$

上面第二个等号之所以成立, 是因为

$$h_{\langle l+N\rangle_N}=h_{\langle l\rangle_N},\qquad \alpha^{k(m+l+N)}=\alpha^{k(m+l)}$$

的缘故.

再证明必要性. 记

$$Y_k=\sum_{n=0}^{N-1}t_{k,n}y_n=\sum_{n=0}^{N-1}t_{k,n}\left[\sum_{m=0}^{N-1}x_mh_{\langle n-m\rangle_N}\right]$$
$$=\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}x_mh_{\langle n-m\rangle_N}t_{k,n},$$

记 $n-m=l$, 由于

$$h_{\langle l+N\rangle_N}=h_{\langle l\rangle_N}, \qquad t_{k,m+N}=t_{k,m},$$

故

$$Y_k=\sum_{m=0}^{N-1}x_m\left[\sum_{l=-m}^{N-m-1}h_{\langle l\rangle_N}t_{k,l+m}\right]=\sum_{m=0}^{N-1}\sum_{l=0}^{N-1}x_mh_lt_{k,m+l}; \tag{5}$$

而

$$X_k=\sum_{m=0}^{N-1}x_mt_{k,m},$$

$$H_k=\sum_{l=0}^{N-1}h_lt_{k,l}, \tag{6}$$

由假设 $Y_k=X_kH_k \quad (k=0,1,\cdots,N-1)$,

得到

$$\sum_{m=0}^{N-1}\sum_{l=0}^{N-1}x_mh_lt_{k,m+l}=\sum_{m=0}^{N-1}\sum_{l=0}^{N-1}x_mh_lt_{k,m}t_{k,l}.$$

由于序列的任意性，就得到

$$t_{k,m+l}=t_{k,m}\cdot t_{k,l} \quad (k,m,l=0,1,\cdots,N-1); \tag{7}$$

在(7)式中，令 $m=l=0$, 就有

$$t_{k,0}=t_{k,0}^2;$$

在复数域中，就有 $t_{k,0}=0$, 或者 $t_{k,0}=1$.

在 $t_{k,0}=0$ 时，在(7)式中令 $l=0$, 就有

$$t_{k,m}=0 \quad (k,m=0,1,\cdots,N-1).$$

于是变换矩阵 T 就为奇异矩阵，我们不讨论这种情况.

在 $t_{k,0}=1(k=0,1,\cdots,N-1)$ 时，T 的第一列元素皆为 1. 在(7)式中令 $m=l=1$, 就得到

$$t_{k,2}=t_{k,1}\cdot t_{k,1}=t_{k,1}^2;$$

令 $m=2$, $l=1$, 就得到

$$t_{k,3}=t_{k,2}\cdot t_{k,1}=t_{k,1}^3;$$

继续之，一般地就得到

$$t_{k,m}=t_{k,1}^m \quad (m,k=0,1,\cdots,N-1). \tag{8}$$

由于 $t_{k,N}=t_{k,0}=1, \quad t_{k,N}=t_{k,N-1+1}=t_{k,N-1}\cdot t_{k,1}$,

故有

$$t_{k,N-1}\cdot t_{k,1}=t_{k,1}^{N-1}\cdot t_{k,1}=t_{k,1}^N=1.$$

这样，由(8)式，就有

$$t_{k,m}^N=(t_{k,1}^m)^N=(t_{k,1}^N)^m=1.$$

即

$$t_{k,m}^N=1$$

$$(k,\ m=0,\ 1,\ \cdots,\ N-1). \tag{9}$$

这就表明 $t_{k,m}$ 必须是 N 次单位根.

由于 T 是非奇异的，故 T 的任意两列(或两行)的元素不能相同. 从而 T 的第二列的各元素 $t_{k,1}$ 的任两个不能相同. 否则，不妨设 $t_{0,1}=t_{1,1}$，这样由(8)式，有 $t_{0,m}=t_{0,1}^m$，$t_{1,m}=t_{1,1}^m$，从而就有 $t_{0,m}=t_{1,m}(m=0,\ 1,\ \cdots,\ N-1)$. 这表示 T 的第一行元素和第二行元素相同，T 就是奇异矩阵了. 又由于在复数域中只有 N 个不同的 N 次单位根，如记 α 为 N 阶单位根(即 N 是使 $\alpha^N=1$ 成立的最小正整数)，其余的 N 次单位根就分别为 $1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \cdots,\ \alpha^{N-1}$. 不失一般性，可取 $t_{1,1}=\alpha$，从而取

$$t_{k,1}=\alpha^k$$

$$(k=0,\ 1,\ \cdots,\ N-1), \tag{10}$$

这就是 T 的第二列元素.

由(8)和(10)，就得到

$$t_{k,m}=t_{k,1}^m=\alpha^{mk}$$

$$(k,\ m=0,\ 1,\ \cdots,\ N-1). \tag{11}$$

这就证明了，如果 T 具有循环卷积特性，T 必为(4)式所示.

证毕.

定理 2 具有(4)式结构的变换是可逆的.

以

$$\tilde{t}_{k,m}=N^{-1}\alpha^{-km}$$

$$(k,\ m=0,\ 1,\ \cdots,\ N-1) \tag{12}$$

为元素的矩阵 U 是 T 的逆矩阵，即 $TU=UT=I$. 其中 I 为单位矩阵.

证明

$$U=N^{-1}\begin{bmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(N-1)}\\ 1 & \alpha^{-2} & \alpha^{-4} & \cdots & \alpha^{-2(N-1)}\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ 1 & \alpha^{-(N-1)} & \alpha^{-2(N-1)} & \cdots & \alpha^{-(N-1)^2}\end{bmatrix}.$$

欲证明 $TU=UT=I$, 只需证明

$$N^{-1}\sum_{m=0}^{N-1}\alpha^{mk}\cdot\alpha^{-nm}=\delta_{kn}=\begin{cases}1, & k\equiv n\,(\mathrm{mod}N),\\ 0, & k\not\equiv n\,(\mathrm{mod}N).\end{cases}$$

在上式中取 $p=k-n$, 就成为

$$N^{-1}\sum_{m=0}^{N-1}\alpha^{mp}=\begin{cases}1, & p\equiv 0\,(\mathrm{mod}N),\\ 0, & p\not\equiv 0\,(\mathrm{mod}N).\end{cases}$$

当 $p\equiv 0(\mathrm{mod}N)$ 时, 有 $\alpha^{mkN}=1(m=0,\ 1,\ \cdots,\ N-1)$, 从而上式第一部分成立. 当 $p\not\equiv 0\,(\mathrm{mod}N)$ 时, 设 $p=kN+l$ $(1\leqslant l\leqslant N-1,\ k$ 为整数), 于是

$$N^{-1}\sum_{m=0}^{N-1}\alpha^{mp}=N^{-1}\sum_{m=0}^{N-1}\alpha^{m(kN+l)}=N^{-1}\sum_{m=0}^{N-1}\alpha^{ml},$$

因此, 只需证明

$$\sum_{m=0}^{N-1}\alpha^{ml}=0\quad(l=1,\ 2,\ \cdots,\ N-1).$$

由于

$$(\alpha^{l}-1)\sum_{m=0}^{N-1}\alpha^{ml}=\alpha^{lN}-1=0\quad(l=1,\ 2,\ \cdots,\ N-1).$$

又由于 $\alpha^{l}-1\neq 0(l=1,\ 2,\ \cdots,\ N-1)$, 故有

$$\sum_{m=0}^{N-1}\alpha^{ml}=0\quad(l=1,\ 2,\ \cdots,\ N-1).\qquad \text{证毕.}$$

推论 1 在复数域中, 只有 DFT 才具有循环卷积特性.

由定理 1 和定理 2 知, 在复数域中, 具有循环卷积特性的变换的唯一结构是:

$$T=\begin{bmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{N-1}\\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(N-1)}\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ 1 & \alpha^{N-1} & \alpha^{2(N-1)} & \cdots & \alpha^{(N-1)^2}\end{bmatrix}, \tag{13}$$

$$T^{-1}=N^{-1}\begin{bmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(N-1)}\\ 1 & \alpha^{-2} & \alpha^{-4} & \cdots & \alpha^{-2(N-1)}\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ 1 & \alpha^{-(N-1)} & \alpha^{-2(N-1)} & \cdots & \alpha^{-(N-1)^2}\end{bmatrix},$$

其中 α 是复数域上的任一 N 阶单位根，通常取

$$\alpha=e^{-j\frac{2\pi}{N}}=W_N,$$

此即 DFT．当取其它的 N 阶单位根时，如

$$\alpha=e^{-j\frac{k2\pi}{N}},\quad (k,N)=1,$$

这时的变换矩阵 T' 与 DFT 的 T 仅行的顺序有差别．因此，如果不计这个差异，则在复数域中，只有 DFT 才具有循环卷积特性．

推论 2 具有(4)式结构的变换是正交变换．

T 的行矢量记作 $\varphi_m(m=0,1,\cdots,N-1)$，那么

$$\left.\begin{aligned}\varphi_0&=(1,1,1,\cdots,1),\\ \varphi_1&=(1,\alpha,\alpha^2,\cdots,\alpha^{N-1}),\\ &\cdots\cdots\cdots\cdots\\ \varphi_m&=(1,\alpha^m,\alpha^{2m},\cdots,\alpha^{m(N-1)}),\\ &\cdots\cdots\cdots\cdots\\ \varphi_{N-1}&=(1,\alpha^{N-1},\alpha^{2(N-1)},\cdots,\alpha^{(N-1)^2}).\end{aligned}\right\} \tag{14}$$

称 φ_m 为变换 T 的基函数. 两个基函数 φ_n, φ_m 的内积定义作*:

$$\langle\varphi_n,\ \varphi_m\rangle=\sum_{k=0}^{N-1}\varphi_n(k)\varphi_m^{-1}(k). \tag{15}$$

根据这个定义及定理 2, 有

$$\begin{aligned}\langle\varphi_n,\ \varphi_m\rangle&=\sum_{k=0}^{N-1}\alpha^{nk}\alpha^{-mk}\\&=\sum_{k=0}^{N-1}\alpha^{k(n-m)}=\begin{cases}N, & m\equiv n(\bmod N),\\0, & m\not\equiv n(\bmod N).\end{cases}\end{aligned}$$

这表示基函数系 $\{\varphi_m(k)\}$ $(m,\ k=0,\ 1,\ \cdots,\ N-1)$ 是正交函数系. 即(4)式的变换是正交变换.

本节的定理 1 和定理 2 是在复数域上证明的, 它说明了 DFT 具有循环卷积特性; 反之, 具有循环卷积特性的变换必为 DFT (除去行的排列顺序的差异外). 因此, 在复数域上, 不存在既具有循环卷积特性、基本函数又比 $W_N=e^{-j\frac{2\pi}{N}}$ 简单的变换. 换句话说, 基本函数是 $W_N=e^{-j\frac{2\pi}{N}}$ 的 DFT 是复数域中具有循环卷积特性的最简单的变换. 但是,

$$W_N=e^{-j\frac{2\pi}{N}}=\cos\frac{2\pi}{N}-j\sin\frac{2\pi}{N},$$

其实部与虚部一般是无理数, 由于运算时位数有限, 不可避免地会带来误差, 与 W_N 及其方幂的乘法也是很麻烦的. 因此, 如果想改进由于 DFT 的基本函数太复杂而带来的一系列缺点, 首先必需在其它数域或数环中来讨论. 序列 x_n 和 h_n 可以认为是整数序列(在数字信号处理中, 输入、输出及匹配滤波器的单位脉冲响应均可当作有界的整数, 这只需把最小的

---

* 两个复矢量 $V=(V_0,\ V_1,\ \cdots,\ V_{N-1})$, $U=(U_0,\ U_1,\cdots,U_{N-1})$ 的内积定义为 $\langle V,\ U\rangle=\sum_{k=0}^{N-1}V_k\cdot\overline{U}_k$.

单位取作 1)，从而想到以正整数 M 为模的剩余类环(域) Z_M. 在整数环（域）Z_M 上能否构造出具有循环卷积特性、基本函数又比 $W_N = e^{-j\frac{2\pi}{N}}$ 简单的变换呢？回答是肯定的.

我们不对一般的具有单位元素的可交换环 R 来讨论具有循环卷积特性的变换的结构，只指出，在 Z_M 上，α 只要满足一定的条件(参阅 **4**)，定理 1 中的变换 T 仍具有循环卷积特性，并且还是可逆的，其逆变换 T^{-1} 就是定理 2 中的 U. 这些正是本书后面要讲到的数论变换的内容.

为了更好的使读者理解数论变换，下一节较详细的介绍一些本书以后要用到的初等数论的基本知识. 一些基本定理的证明，如果不是太复杂，也尽量给出，以便读者阅读.

— 3 —

数论的基本知识

一、整数的整除性

1. 设a, b是任意两个整数，$b\neq 0$，如果存在一个整数q，使得等式$a=bq$成立，就说b整除a，记作$b|a$. b是a的因数（或约数），a是b的倍数. 如果不存在整数q使等式$a=bq$成立，那么就说b不能整除a，记作$b\nmid a$.

显然有

1° $a|a$, $1|a$, 其中a为任意整数.

2° 如果$a|b$, $b|a$, 那么$a=\pm b$.

3° 如果$b|a$, $c|b$, 那么$c|a$（传递性）.

4° 如果$c|a$, $c|b$, 那么$c|a\pm b$.

5° 如果$c|a$, 那么$c|ab$.

其中a, b, c均为整数.

6° 设a, b是任意整数，$b>0$，则存在两个唯一的整数q和r，使得等式$a=bq+r$成立（$0\leqslant r<b$），r称为整数a模b的最小非负剩余，记为$\langle a\rangle_b$. 其中q叫做“不完全商数”，或简称为“商数”. 显然，如果$r=0$，则$b|a$，如果$r\neq 0$，则$b\nmid a$.

上述结论中的q和r的唯一性可用反证法来证明，至于q和r的存在性是很明显的.

设
$$a=bq+r,$$
$$a=bq_1+r_1,$$
其中，$0\leqslant r<b$, $0\leqslant r_1<b$. 后式减去前式，得

$$b(q-q_1)+(r-r_1)=0,$$

即
$$b(q-q_1)=-(r-r_1).$$

如果 $r\neq r_1$, 不妨设 $r>r_1$, 于是 $0<r-r_1<b$. 但上式的左边是 b 的倍数, 故有 $b|r-r_1$. 但这与 $0<r-r_1<b$ 矛盾, 从而 $r=r_1$. 于是 $q=q_1$.

2. 设 $a_1, a_2, \cdots, a_n$ 是 n 个整数 $(n\geqslant 2)$, 若整数 d 是它们之中每一个的约数, 那么 d 就叫做 $a_1, a_2, \cdots, a_n$ 的一个公约数, 所有公约数中最大的一个叫做最大公约数, 记作$(a_1, a_2, \cdots, a_n)$. 如果$(a_1, a_2, \cdots, a_n)=1$, 我们就说 $a_1, a_2, \cdots, a_n$ 互素. 如果对任意两个 a_i 与 $a_j(1\leqslant i, j\leqslant n)$, 有 $(a_i, a_j)=1$, 我们就说 $a_1, a_2, \cdots, a_n$ 两两互素. 如果 m 是 $a_1, a_2, \cdots, a_n$ 这 n 个数的倍数, 就称m是这 n 个数的公倍数, 所有公倍数中最小的正数叫做最小公倍数, 记作$[a_1, a_2, \cdots, a_n]$. 显然, 如果正整数 $a_1, a_2, \cdots, a_n$ 两两互素, 则

$$[a_1, a_2, \cdots, a_n]=a_1a_2\cdots a_n.$$

关于最大公约数, 有如下事实:

1° 如果 a 是 b 的倍数, 则 a 和 b 的公约数的集合与 b 的约数的集合重合, 特别$(a, b)=b$.

2° 如果 $a=bq+r$, $b\neq 0$, 则$(a, b)=(b, r)$.

实际上, 由 $a=bq+r$ 可知, a 和 b 的每一个公约数也除尽 r. 反之, b 和 r 的公约数除尽 a, 从而也是 a 和 b 的公约数, 所以 a, b 的公约数的集合与 b, r 的公约数的集合相同. 从而$(a, b)=(b, r)$.

3° 设m表示任意正整数, 则$(am, bm)=m(a, b)$.

4° 设$(a, b)=d$, 则 $\left(\frac{a}{d}, \frac{b}{d}\right)=1$. 也就是说, 两个数被它们的最大公约数除得的商数是互素的.

事实上，由 3° 可知

$$(a,\ b)=\left(\frac{a}{d}d,\ \frac{b}{d}d\right)=\left(\frac{a}{d},\ \frac{b}{d}\right)d,$$

故

$$\left(\frac{a}{d},\ \frac{b}{d}\right)=1.$$

5° 如果$(a,\ b)=1$，则$(ac,\ b)=(c,\ b)$.

这是由于$(ac,\ b)$是 ac 和 bc 的公约数，由于 a 和 b 互素，故$(ac,\ b)$除尽 c，显然$(ac,\ b)$除尽 b，故$(ac,\ b)\mid(c,\ b)$. 反之，显然有$(c,\ b)\mid(ac,\ b)$，所以$(ac,\ b)=(c,\ b)$.

6° 如果$(a,\ b)=1$，且 $b\mid ac$，则 $b\mid c$.

由 5° 知$(ac,\ b)=(c,\ b)$，由 1° 知$(ac,\ b)=b$. 所以 $b\mid c$.

7° 如果 $a_1,\ a_2,\ \cdots,\ a_m$ 中的每一个与 $b_1,\ b_2,\ \cdots,\ b_n$ 中的每一个互素，则$(a_1a_2\cdots a_m,\ b_1b_2\cdots b_n)=1$.

实际上，由 5° 知，

$$\begin{aligned}(a_1a_2a_3\cdots a_m,\ b_k)&=(a_2a_3\cdots a_m,\ b_k)=(a_3\cdots a_m,\ b_k)=\cdots\\&=(a_m,\ b_k)=1\quad(k=1,\ 2,\ \cdots,\ n),\end{aligned}$$

故若记 $A=a_1a_2\cdots a_m$，有

$$(b_1b_2\cdots b_n,\ A)=(b_2\cdots b_n,\ A)=\cdots=(b_n,\ A)=1.$$

8° 两正整数 a，b 互素的充要条件是存在两个整数 m，n，使

$$am+bn=1.$$

这一事实可用欧几里得辗转相除法证明，或者证明不定方程 $ax+by=1$ 有整数解的充要条件是 $(a,\ b)=1$.

9° 如果$(a,\ c)=1$，$(b,\ c)=1$，则$(ab,\ c)=1$.

由于$(a,\ c)=1$，$(b,\ c)=1$，故根据 8°，有

$$am_1+cn_1=1,\qquad bm_2+cn_2=1,$$

两式相乘，即得

$$abm+cn=1.$$

其中，$m=m_1m_2$，$n=bm_2n_1+am_1n_2+cn_1n_2$，均为整数，故由 8° 知，$(ab, c)=1$.

特别，当$(a, c)=1$时，$(a^n, c)=1$. 其中 n 是正整数.

3. 一个大于 1 的整数，如果它的正约数只有 1 和它本身，就叫做素数，如 2, 3, 5, 7 等都是素数（2 是唯一的偶素数），否则就叫做复合数.

1° 设整数 $a>1$，则 a 的大于 1 的最小约数是素数.

这是因为如果 a 的大于 1 的最小约数 q 是复合数，那么 q 的某个不为 1 的约数 $q_1(1<q_1<q)$ 必为 a 的约数，但这与 q 的性质矛盾.

2° 设 p 是素数，则对任一整数 a，或者$(a, p)=1$，或者 $p|a$，二者必居其一.

事实上，由于$(a, p)|p$，而 p 是素数，所以$(a, p)=1$，或者$(a, p)=p$. 在后一种情形下，$p|a$.

3° 设 p 是素数，如果 $p|a_1\cdot a_2\cdot\cdots\cdot a_n$，则 p 至少能除尽一个 $a_k(1\leqslant k\leqslant n)$.

这是直接由 2° 得到的. 事实上，每一个 a_k 或者被 p 除尽，或者与 p 互素. 如果所有的 $a_k(k=1, 2, \cdots, n)$ 均与 p 互素，那么 p 与 $a_1a_2\cdots a_n$ 互素，这与 $p|a_1a_2\cdots a_n$ 矛盾. 所以至少有一个 a_k 被 p 除尽.

4° 任一个大于 1 的整数 M 能够唯一地分解作

$$M=p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s}, \tag{1}$$

其中，$l_i(i=1, 2, \cdots, s)$是正整数，$p_i(i=1, 2, \cdots, s)$是素数，$p_1<p_2<\cdots<p_s$. 这叫做 M 的标准分解式.

事实上，设 p_1 是 M 的最小素约数，有 $M=p_1M_1$. 如果 $M_1>1$，用 p_1' 表示 M_1 的最小素约数，有 $M_1=p_1'M_2$. 如果

$M_2>1$, 同样可得到 $M_2=p'_2M_3$. 继续之, 直到 $M_n=1$ 为止, 这时有 $M_{n-1}=p'_{n-1}$. 这样便有了 M 的一个素因子分解式:

$$M=p_1p'_1p'_2\cdots p'_{n-1}.$$

如果还有另一个素因子分解式 $M=q_1q'_1q'_2\cdots q'_{m-1}$, 则

$$p_1p'_1p'_2\cdots p'_{n-1}=q_1q'_1q'_2\cdots q'_{m-1}.$$

等号右边可被 q_1 除尽,因此由 3° 知,左边至少有一个因子被 q_1 除尽,不妨设这个因子为 p_1, 从而 $p_1=q_1$, 在上等式中两边约去 p_1, q_1. 这样就有

$$p'_1p'_2\cdots p'_{n-1}=q'_1q'_2\cdots q'_{m-1}.$$

对这个等式重复应用上面的推论, 直到将右边所有的因子全部约掉为止. 这时左边的因子也同时全部约掉了, 否则就有 $p'_m\cdots p'_{n-1}=1$. 这对于均大于 1 的整数 p'_k $(m\leqslant k\leqslant n-1)$ 是不可能成立的.

最后将 $M=p_1p'_1p'_2\cdots p'_{n-1}$ 中相同的素因子合并, 就得到标准分解式(1).

例 1 设 n 为大于 1 的整数, $n!=1\cdot2\cdot3\cdots n$ 的标准分解式为

$$n!=\prod_i p_i^{\sum_{\lambda=1}^{\infty}\left[\frac{n}{p_i^\lambda}\right]}.$$

其中, p_i 为小于 n 的素数, $\sum_{\lambda=1}^{\infty}\left[\frac{n}{p_i^\lambda}\right]$为 p_i 的方幂. $[x]$表示不超过 x 的最大整数, 例如[7]=7, [2.6]=2, [−4.75]=−5 等.

这个阶乘的标准分解式我们不加以证明, 读者可参考文献[10],这里举一例子说明该分解式的应用.

将 25! 分解成素约数之积.

【解】 写出比 25 小的一切素数

$$2, 3, 5, 7, 11, 13, 17, 19, 23.$$

然后用这些数及其幂去除 25，写出整商部分，得出下表.

整　商	素								数
	2	3	5	7	11	13	17	19	23
$\left[\frac{25}{p}\right]$	12	8	5	3	2	1	1	1	1
$\left[\frac{25}{p^2}\right]$	6	2	1						
$\left[\frac{25}{p^3}\right]$	3								
$\left[\frac{25}{p^4}\right]$	1								
相　加	22	10	6	3	2	1	1	1	1

故 $$25! = 2^{22}\cdot 3^{10}\cdot 5^6\cdot 7^3\cdot 11^2\cdot 13\cdot 17\cdot 19\cdot 23.$$

二、关于以正整数 M 为模的整数环 Z_M 的概念

定义 1　如果两个整数 a, b 被一正整数 M 所除得的余数相等，则称 a, b 模 M 同余（等余），记作

$$a \equiv b \pmod{M}.$$

由定义显然有

1° 整数 a 与 b 模 M 同余的充要条件是 $M \mid a-b$.

2° 若 $a \equiv b \pmod{M}$，则 $b \equiv a \pmod{M}$.

3° 若 $a \equiv b \pmod{M}$，$b \equiv c \pmod{M}$，则 $a \equiv c \pmod{M}$.

4° 若 $a \equiv b \pmod{M}$，则 $a \pm c \equiv b \pm c \pmod{M}$，

$ac \equiv bc \pmod{M}$，其中 c 为任一整数.

5° 若 $a\equiv b(\bmod M)$, $c\equiv d(\bmod M)$, 则

$$a\pm c\equiv b\pm d(\bmod M),\quad ac\equiv bd(\bmod M).$$

6° 若 $ac\equiv bc(\bmod M)$, 且 $(c, M)=1$ (即 c 和 M 互素), 则 $a\equiv b(\bmod M)$.

7° 若 $a\equiv b(\bmod m_i)$ $(i=1, 2, \cdots, s)$, 则

$$a\equiv b(\bmod [m_1, m_2, \cdots, m_s]).$$

8° 若 $a\equiv b(\bmod M)$, $d|M$, $d>0$, 则 $a\equiv b(\bmod d)$.

9° 若 $a\equiv b(\bmod M)$, 则 $(a, M)=(b, M)$. 因而, 若 d 能整除 M 及 a, b 二数之一者, 则 d 必能整除 a, b 中的另一个.

10° 若 $a\equiv b(\bmod M)$, d 是 a, b 及 M 的任一正公因数, 则

$$\frac{a}{d}\equiv\frac{b}{d}\left(\bmod \frac{M}{d}\right).$$

以上事实 1°~10° 均不难用定义 1 加以证明. 例如 1°, 由于 $a\equiv b$ $(\bmod M)$, 故 $a=b+kM$, 其中 k 为整数. 所以 $a-b=kM$, 这表示 $M|a-b$. 反之, 如果 $M|a-b$, 则 $a-b=kM$ (k 为整数), 这表示 $a\equiv b(\bmod M)$. 因此 $a\equiv b(\bmod M)$ 等价于 $M|a-b$.

又如 9°, 由 $a\equiv b$ $(\bmod M)$, 有 $a=b+kM$ (k 为整数). 根据上一段 2-2°, 有 $(a, M)=(b, M)$. 因此, 如果 a 和 M 互素, 则 b 也和 M 互素.

再如 6°, 由 $ac\equiv bc(\bmod M)$, 故 $M|ac-bc$, 即 $M|c(a-b)$, 由于 M 与 c 互素, $M\nmid c$, 故必 $M|a-b$, 故

$$a\equiv b(\bmod M).$$

这里读者特别要注意, 如果 c 与 M 不互素, 那么虽然有

$$ac\equiv bc(\bmod M),$$

但未必成立 $a\equiv b$ $(\bmod M)$. 例如 $2\cdot5\equiv4\cdot5$ $(\bmod 10)$, 由于

$(5, 10)=5\neq 1$, 故有 $2\not\equiv 4 \pmod{10}$. 这里一般有如下事实: 若 $ac\equiv bc \pmod M$, 而 $(c, M)=d$, 则 $a\equiv b \left(\bmod \dfrac{M}{d}\right)$.

同余运算是数论变换的基本运算, 读者务必注意.

定义 2 对全体整数以 M 为模分成若干类, 将对模 M 同余的整数归为一类, 叫做模 M 的同余类, 于是就将全体整数划为 M 类. 从每一类中取出一数作为代表, 这样选出的 M 个数所成的集叫做以 M 为模的完全剩余系. 如 $\{0, 1, \cdots, M-1\}$ 就是以 M 为模的完全剩余系. 由于这是从每一类中取出的最小的非负整数, 所以称之为非负最小完全剩余系, 记作 Z_M.

以后各节中, Z_M 均指

$$Z_M=\{0, 1, \cdots, M-1\}.$$

在完全剩余系 Z_M 中, 加法和乘法的意义如下:

设 $k, l\in Z_M$.

加法: 当 $k+l<M$ 时, $k+l=k+l$;

当 $k+l\geqslant M$ 时, $k+l=k+l-M$.

乘法: $kl=r$, 其中 $kl=qM+r$, $0\leqslant r<M$, q 为整数.

这样的加法及乘法也可表作

$$k+l\equiv k+l-M \pmod M,$$

$$kl\equiv r \pmod M.$$

在代数中, 如果一个数系对于加法(减法)和乘法是封闭的(当然加法和乘法还必需满足交换律、结合律及分配律等运算法则), 就称这个数系为数环(这里指交换环). 由于在 Z_M 上定义了加法和乘法, 不难验证这样定义的加法和乘法是满足交换律、结合律及分配律的, 并且 Z_M 对于加法和乘法是封闭的, 故 Z_M 是一个数环, 称为以 M 为模的整数环. 这里

Z_M 对于加法和乘法是封闭的，是指 Z_M 中的任何两个元素作加法和乘法(按上面所定义的加法和乘法)，其结果仍为 Z_M 中的元素.

Z_M 是有单位元素的环，1 是它的单位元素，0 是它的零元素．对于 $a\neq 0$，且 $a\in Z_M$，存在 Z_M 中的 b，使 $a+b=0$，b 叫做 a 的负元素，记作 $-a$.

取负：$-k=M-k$.

减法：$k-l=k+(-l)$.

例 2 设 $M=7$．$Z_M=\{0, 1, 2, 3, 4, 5, 6\}$.

加法：$1+3=4$，$5+6=4$.

乘法：$4\cdot 5=6$，$2\cdot 3=6$.

取负：$-5=7-5=2$

减法：$3-5=3+(-5)=3+2=5$.

从上定义可知，Z_M 中的加法(减法)和乘法就是通常正整数模 M 的加法和乘法.

设 $a\in Z_M$，$a\neq 0$，如果存在 $b\in Z_M$，$b\neq 0$，使得 $ab=1$，则称 b 为 a 的逆元素，简称逆元，记作 a^{-1}(显然，a 亦为 b 的逆元)．例如，在例 2 中，由于 $2\cdot 4\equiv 1 \pmod 7$，$3\cdot 5\equiv 1 \pmod 7$，$6\cdot 6\equiv 1 \pmod 7$，故 $2^{-1}=4$，$3^{-1}=5$，$4^{-1}=2$，$5^{-1}=3$，$6^{-1}=6$，$1^{-1}=1$．亦即，Z_7 中除零元素 0 外，每个元素都有逆元．但当 $M=6$，$Z_6=\{0, 1, 2, 3, 4, 5\}$ 中，除去 1 和 5 有逆元外，2，3，4 均无逆元.

定理 1 设 $a\in Z_M$，$a\neq 0$，在 Z_M 中存在逆元 a^{-1} 的充要条件是 $(a, M)=1$.

证明 充分性.

设 $(a, M)=1$，这时存在整数 m，n，使

$$am+nM=1$$

于是 $am-1=(-n)M$, 亦即 $am\equiv 1(\bmod M)$. m 即为 a^{-1}.

必要性.

设 $a^{-1}a\equiv 1\ (\bmod M)$. 那么 $a^{-1}a=1+mM$ (m 为整数), 故 $a^{-1}a+(-m)M=1$, 这表示 $(a,\ M)=1$, 即 a 与 M 互素.

推论 1 如果 M 为素数, 则 Z_M 中每一个非零元素均有逆元.

这是因为 Z_M 中每一个非零元素均与 M 互素的缘故.

推论 2 如果 M 为一素数, 则 Z_M 为一整数域, 称为以正整数 M 为模的整数域. 在这种情况下, 设 $a,\ b\in Z_M,\ b\neq 0$, $\frac{a}{b}=ab^{-1}$.

在代数上, 称一交换环为域(或体), 是指这个环至少有一个非零元素, 并且对于它的任一非零元素都存在逆元. 这里当 M 是素数时, 根据推论 1, Z_M 中每一个非零元素都有逆元, 故这时, Z_M 为域.

三、Euler 函数及 Euler、Fermat 定理

定义 3 给定正整数 M, 不大于 M 并与 M 互素的正整数的个数记作 $\varphi(M)$, 称 $\varphi(M)$ 为 Euler 函数.

例如, $\varphi(1)=1,\ \varphi(2)=1,\ \varphi(3)=2,\ \varphi(p)=p-1$ (p 设为素数).

定理 2 如果将 M 分解为素数因子的乘积 $M=p_1^{l_1}\cdot p_2^{l_2}\cdots p_s^{l_s}$ (l_i 为正整数, p_i 为互异素数), 则

$$\varphi(M)=M\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_s}\right).$$

例如, $M=12=2^2\cdot 3$, 则

$$\varphi(12)=12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=4.$$

推论 1 如果 M 是素数，则

$$\varphi(M)=M-1.$$

推论 2 若 μ 和 ν 是任意两个互素的正整数，则

$$\varphi(\mu\nu)=\varphi(\mu)\cdot\varphi(\nu).$$

这只要对正整数 $\mu\nu$, μ, ν 分别利用定理 2，并注意 μ, ν 没有相同的素因子即可得到.

定理 3 就自然数 M 的一切约数作 Euler 函数，则这些所作的诸 Euler 函数之和等于 M，即

$$\sum_i \varphi(\alpha_i)=M, \quad 其中\ \alpha_i \mid M.$$

例如，$M=12$，其约数为 1, 2, 3, 4, 6, 12. 有

$$\begin{aligned}&\varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12)\\&=1+1+2+2+2+4=12.\end{aligned}$$

定理 4 (Euler 定理)设 M 为任一自然数，a 为与 M 互素的任意整数，$(a, M)=1$，则 $a^{\varphi(M)}-1$ 可为 M 除尽，即

$$a^{\varphi(M)}\equiv 1 \pmod{M}.$$

定理 5 (Fermat 定理)若 p 为一素数，a 为与 p 互素的任意整数，则 $a^{p-1}-1$ 可为 p 除尽，即

$$a^{p-1}\equiv 1 \pmod{p}.$$

这是由于在 $M=p$ 为素数时，$\varphi(p)=p-1$ 的缘故.

Fermat 定理在数论变换的证明中经常用到. 下面给出一个不利用 Euler 定理的证明. 显然

$$(a+1)^p\equiv a^p+1 \pmod{p}.$$

两端同时减去 $a+1$，有

$$(a+1)^p-(a+1)\equiv a^p-a \pmod{p}.$$

由此知，如果 $p|a^p-a$，则 $p|(a+1)^p-(a+1)$．显然有 $p|1^p-1$，故 $p|2^p-2$，…，因此，一般地成立 $p|a^p-a$，即

$$a^p \equiv a \pmod{p},$$

由于 $(a, p)=1$，故

$$a^{p-1} \equiv 1 \pmod{p}.$$

推论 设 p 为素数，a 与 p 互素，则

$$a^{\frac{p-1}{2}}+1, \quad a^{\frac{p-1}{2}}-1$$

中必有一个为 p 的倍数．即

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \quad 或 \quad a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

二者必居其一．

四、孙子定理

设 $a_1, a_2, a_3, \cdots, a_k$ 为整数，$m_1, m_2, \cdots, m_k$ 为正整数，称

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\cdots\cdots\cdots\cdots \\ x &\equiv a_k \pmod{m_k} \end{aligned} \qquad (**)$$

为联立一次同余方程组．如果有一整数 l，使得

$$\begin{aligned} l &\equiv a_1 \pmod{m_1}, \\ l &\equiv a_2 \pmod{m_2}, \\ &\cdots\cdots\cdots\cdots \\ l &\equiv a_k \pmod{m_k} \end{aligned}$$

成立，则称 l 为联立同余方程组的解（或根）．求同余方程的解，叫做解同余方程．

定理 6（孙子定理） 设 $m_1, m_2, \cdots, m_k$ 为两两互素的 k

个正整数，$m=m_1\cdot m_2\cdots m_k$，$m=m_iM_i$，$i=1,2,\cdots,k$，则同余方程组(**)的解是

$$x\equiv M_1'M_1a_1+M_2'M_2a_2+\cdots+M_k'M_ka_k \pmod{m}.$$

其中，$M_i'M_i\equiv 1 \pmod{m_i}$，$i=1,2,\cdots,k$.

例 3 解同余方程组

$$\begin{cases} x\equiv 1 \pmod{5}, \\ x\equiv 5 \pmod{6}, \\ x\equiv 4 \pmod{7}, \\ x\equiv 10 \pmod{11}. \end{cases}$$

【解】 此时，$m=5\cdot6\cdot7\cdot11=2310$，$M_1=6\cdot7\cdot11=462$，$M_2=5\cdot7\cdot11=385$，$M_3=5\cdot6\cdot11=330$，$M_4=5\cdot6\cdot7=210$.

解同余方程

$$M_i'M_i\equiv 1 \pmod{m_i},\quad i=1,2,3,4.$$

得：$M_1'=3$，$M_2'=1$，$M_3'=1$，$M_4'=1$. 故由孙子定理，解为

$$\begin{aligned} x&\equiv 1\cdot3\cdot462+5\cdot1\cdot385+4\cdot1\cdot330+10\cdot1\cdot210 \\ &\equiv 6731\equiv 2111 \pmod{2310}. \end{aligned}$$

五、以 M 为模的整数环 Z_M 中的单位根

定义 4 设 a 是 Z_M 中的非零元素，如果存在正整数 N，使 $a^N\equiv 1 \pmod{M}$，则称 a 是 Z_M 中的 N 次单位根. 如果 N 是使上式成立的最小正整数，即 $a^N\equiv 1 \pmod{M}$，$a^l\not\equiv 1\,(l=1,2,\cdots,N-1) \pmod{M}$，则称 a 是对模 M 的 N 阶本原单位根，而称 N 是 a 对模 M 的阶数.

如果 a 对模 M 的阶数是 $\varphi(M)$，则称 a 是模 M 或 Z_M 的主根(元根).

例如，$M=10$，$a=3$，由于

$$3^1\equiv 3,\quad 3^2\equiv 9,\quad 3^3\equiv 7,\quad 3^4\equiv 1 \pmod{10},$$

所以 3 是对模 10 的 4 阶单位根，又由于 $\varphi(10)=4$，所以 3 是模 10 的主根.

1° 设 $a\in Z_M$，$a\neq 0$，a 为 Z_M 中的单位根的充要条件是

$$(a,\ M)=1.$$

这是因为，如果 a 与 M 不互素，但 a 为 Z_M 中的单位根，$a^d\equiv 1 \pmod{M}$，$d>1$. 那么就有 $a\cdot a^{d-1}\equiv 1 \pmod{M}$，这表示 a^{d-1} 为 a 在 Z_M 中的逆元，但这与本节定理 1 矛盾. 反之，如果 $(a,\ M)=1$，则由 Euler 定理，有 $a^{\varphi(M)}\equiv 1 \pmod{M}$，这表示 a 是 Z_M 中的单位根（$\varphi(M)$ 次）.

2° 如果 $a\in Z_M$，$a\neq 0$，且为 Z_M 中的单位根，则 a 在 Z_M 中存在逆元 a^{-1}.

这是因为 $(a,\ M)=1$ 的缘故.

3° 如果 a 对模 M 的阶数为 N，则 $1,\ a,\ a^2\cdots a^{N-1}$ 对模 M 两两互不同余.

事实上，如果 $a^l\equiv a^k \pmod{M}$，$0\leqslant k<l<N$，那么就有 $a^{l-k}\equiv 1 \pmod{M}$，$0<l-k<N$，但这与 a 对模 M 的阶为 N 矛盾.

4° 如果 a 对 M 的阶数为 N，又存在另一个正整数 n，使 $a^n\equiv 1 \pmod{M}$，则必有

$$N\mid n.$$

特别

$$N\mid \varphi(M).$$

事实上，若 $n=qN+r$ $(0\leqslant r<N$，q 为整数)，则由于 $a^n\equiv a^{qN+r}\equiv a^r\equiv 1 \pmod{M}$. 由于 a 对模 M 的阶为 N，故 $r=0$. 所以 $n=qN$，这表示 $N\mid n$.

由 4° 可知，要求 a 对模 M 的阶数 N，只要对 $\varphi(M)$ 的正整数约数验证就可以了. 例如，要求 5 对模 12 的阶数，只要

对 5 的 2 次方和 4 次方来试验就可以了，这是因为 $\varphi(12)=4$，它有正整数约数 1, 2, 4. 而 $5^2\equiv1(\bmod 12)$. 故 5 对模 12 的阶数是 2.

推论 设 M 为一素数，a 对模 M 的阶数为 N，则 N 必为 $M-1$ 的约数. 又如果 d 为 $M-1$ 的任一约数，则 Z_M 中以 d 为阶数的正整数的个数为 $\varphi(d)$.

这推论的前一部分可由 4° 直接推得，后一部分证明较困难，这里从略.

5° 设 a 和 b 均和 M 互素，且 $a\equiv b(\bmod M)$，则 a 和 b 对模 M 的阶数相同.

事实上，设 a 和 b 对模 M 的阶分别为 N_1, N_2，由于 $a\equiv b(\bmod M)$，故 $a^{N_1}\equiv b^{N_1}(\bmod M)$，由于 $a^{N_1}\equiv1(\bmod M)$，故 $b^{N_1}\equiv1(\bmod M)$，这表示 $N_2\leqslant N_1$. 同理可证 $N_2\geqslant N_1$，所以 $N_1=N_2$.

6° 如果 a 对模 M 的阶数为 N，又设 $k|N$，那么 a^k 对模 M 的阶数是 $\frac{N}{k}$.

如果 g 为模 M 的主根，则 $a=g^{\frac{\varphi(M)}{N}}$ 对模 M 的阶数是 N. 其中 N 是 $\varphi(M)$ 的任一约数.

7° 设 $M=p_1^{l_1}\cdot p_2^{l_2}\cdots p_s^{l_s}$，$a$ 对模 M 的阶数是 N，对模 $p_i^{l_i}$ 的阶数是 $N_i(i=1, 2, \cdots, s)$，则

$$N=[N_1, N_2, \cdots, N_s].$$

证明：由于 $a^N\equiv1(\bmod M)$，所以有

$$a^N\equiv1(\bmod p_i^{l_i})\quad(i=1, 2, \cdots, s).$$

因此，$N_i|N(i=1, 2, \cdots, s)$. 这表示 N 为 N_1, N_2, $\cdots$, N_s 的公倍数. 下面再证明 N 为 N_1, N_2, $\cdots$, N_s 的最小公倍数 $[N_1, N_2, \cdots, N_s]$.

由于 $N=d[N_1, N_2, \cdots, N_s]$，其中 d 为正整数，所以有

$$a^{\frac{N}{d}}=a^{[N_1,N_2,\cdots,N_s]}=[a^{N_i}]^{\frac{[N_1,N_2\cdots N_s]}{N_i}}$$
$$\equiv 1(\bmod p_i^{l_i})\quad (i=1,\ 2,\ \cdots,\ s),$$

故有
$$a^{\frac{N}{d}}\equiv 1(\bmod M).$$

但是由于 a 对模 M 的阶为 N, 故 $d=1$. 所以
$$N=[N_1,\ N_2\cdots N_s].$$

这表明, 如果 a 对模 $p_i^{l_i}(i=1,\ 2,\ \cdots,\ s)$ 的阶数为 N, 那么 a 对模 M 的阶为 N. 但是反之未必成立, 也就是说, a 对模 M 的阶为 N, 未必对模 $p_i^{l_i}$ 的阶为 N. 例如, $M=15=3\cdot 5$. 2 对模 15 的阶为 4, 但对模 3 的阶为 2, 对模 5 的阶为 4. 显然 $[2,\ 4]=4$.

8° 模 M 有主根的充分必要条件是 $M=2,\ 4,\ p^\alpha,\ 2p^\alpha$, 这里 α 为自然数, p 是奇素数.

为了说明以上所述的概念和性质, 举一例说明之.

例 4 设 $\quad M=7,\ Z_7=\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6\}.$

其中非零元素均与 7 互素, 故均为 Z_M 中的某次单位根. $\varphi(7)=6$, 6 的约数为 1, 2, 3, 6. 故有 $\varphi(1)=1$ 个一阶单位根, 即 1; 有 $\varphi(2)=1$ 个 2 阶单位根, 即 6; 有 $\varphi(3)=2$ 个 3 阶单位根, 即 4 和 2; 有 $\varphi(6)=2$ 个 6 阶单位根(主根), 即 3 和 5. 相加共有 $\varphi(1)+\varphi(2)+\varphi(3)+\varphi(6)=6$ 个. 3 为模 7 的主根, 那么模 7 的 2 阶单位根 $\alpha_2=3^{\frac{7-1}{2}}=3^3\equiv 6$, 模 7 的 3 阶单位根 $\alpha_3=3^{\frac{7-1}{3}}=3^2\equiv 2$, 另一个 3 阶单位根为
$$\alpha_3=5^{\frac{7-1}{3}}=5^2=25\equiv 4.$$

六、勒让德(Legendre)符号

如果如下二次同余方程

$$x^2 \equiv a \pmod{p}, \quad (a, p)=1$$

有整数解，就称 a 是模 p 的平方剩余，否则称 a 为非平方剩余．当 p 是奇素数且 $(a,p)=1$ 时，由 Fermat 定理的推论知

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad 与 \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

二者必居其一．前一种情形，由 $x^{p-1}\equiv 1 \pmod{p}$ 和 $a^{\frac{p-1}{2}}\equiv 1 \pmod{p}$，根据本章二中的 5°、6° 可得 $x^2\equiv a \pmod{p}$，易见 a 是模 p 的平方剩余，后一种情形，易见 a 为非平方剩余．

称
$$\left(\frac{a}{p}\right)$$
为勒让德(Legendre)符号，其中 p 是奇素数．它对所有不是 p 的倍数的整数 a 都有定义．定义它为

$$\left(\frac{a}{p}\right)=\begin{cases} 1, & a\text{是素数}\,p\,\text{的平方剩余}, \\ -1, & a\text{非平方剩余}. \end{cases}$$

有
$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod{p}.$$

于是有如下事实:

1° $\left(\frac{1}{p}\right)=1$.

2° $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

3° 如果 $a\equiv b \pmod{p}$，则 $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

这是因为属于同一类的数同是平方剩余或同是非平方剩余的缘故.

4° 反转律　如果 p 和 q 都是奇素数，则

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

特别，如果 p 和 q 都有形式 $4m+3$，则

$$\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right);$$

而如果 p, q 中有一个有形式 $4m+1$, 则

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right).$$

反转律是非常重要的定理，我们在证明 Fermat 数变换时，将用到它。

—4—

一维数论变换

现在，在 **2** 讨论的基础上，在以正整数 M 为模的整数环(或域) Z_M 上具体建立具有循环卷积特性的可逆变换.

在 Z_M 上给出两个长为 N 的序列 x_n 和 h_n 及其循环卷积 y_n,

$$(x)=\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{N-1} \end{bmatrix}, \qquad (h)=\begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ \vdots \\ h_{N-1} \end{bmatrix},$$

$$y_n=\sum_{k=0}^{N-1} x_k h_{\langle n-k\rangle_N} \quad (n=0,\ 1,\ \cdots,\ N-1).$$

考虑可逆变换 T，作变换

$$(X)\equiv T(x)\,(\mathrm{mod}M),$$
$$(H)\equiv T(h)\,(\mathrm{mod}M),$$
$$(Y)\equiv T(y)\,(\mathrm{mod}M).$$

完全同 **2** 中的讨论，欲使 T 具有循环卷积特性

$$Y_k\equiv X_k H_k(\mathrm{mod}M) \quad (k=0,\ 1,\ \cdots,\ N-1),$$

只须 T 具有结构

$$T\equiv\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{N-1} & \alpha^{2(N-1)} & \cdots & \alpha^{(N-1)^2} \end{bmatrix}(\mathrm{mod}M),$$

其中 α 取作模 M 的 N 阶本原单位根.

下面我们来证明，当 $M=p_1^{l_1}\cdot p_2^{l_2}\cdots p_s^{l_s}$ 时，α 不仅对模 M 的阶数为 N，而且对模 $p_i(i=1, 2, \cdots, s)$ 的阶数亦为 N 时，下列一对变换互为逆变换.

设 $x_n\in Z_M\ (n=0, 1, 2, \cdots, N-1)$，则称

$$X_k\equiv\sum_{n=0}^{N-1}x_n\alpha^{nk}(\bmod M)\quad(k=0, 1, \cdots, N-1),\tag{1}$$

$$x_n\equiv N^{-1}\sum_{k=0}^{N-1}X_k\alpha^{-nk}(\bmod M)\quad(n=0, 1, \cdots, N-1)\tag{2}$$

为数论变换(NTT). 其中 $\alpha\in Z_M$. 不妨设 $N\geqslant 2$.

定理1 设 $M=p_1^{l_1}\cdot p_2^{l_2}\cdots p_s^{l_s}$，当且仅当

1° N^{-1} 在 Z_M 上存在，即 $(N, M)=1$;

2° α 对模 M 是 N 阶本原单位根;

3° α 对模 $p_i(i=1, 2, \cdots, s)$ 的阶数亦为 N 时，(1)与(2)为一对互逆变换. 如果 M 是素数，则条件2°包含条件3°.

证明 欲使(2)成立，必须 N^{-1} 在 Z_M 上存在，即

$$(N, M)=1.$$

将(2)代入(1)，得

$$X_k\equiv\sum_{m=0}^{N-1}X_m\left(N^{-1}\sum_{n=0}^{N-1}\alpha^{n(k-m)}\right)(\bmod M).$$

欲证明(1)与(2)为一对互逆变换，必须且只需有

$$N^{-1}\sum_{n=0}^{N-1}\alpha^{n(k-m)}\equiv\begin{cases}1, & k-m\equiv 0\ (\bmod N)\\ 0, & k-m\not\equiv 0\ (\bmod N)\end{cases}(\bmod M).$$

若记 $j=k-m$，则(1)与(2)为互逆变换的充要条件为

$$N^{-1}\sum_{n=0}^{N-1}\alpha^{nj}\equiv\begin{cases}1, & j\equiv 0(\bmod N)\\ 0, & j=1,2,\cdots,N-1\end{cases}\quad(\bmod M).\tag{3}$$

现设(1)与(2)为一对互逆变换，显然 N^{-1} 在 Z_M 存在，且

(3)式成立. 这时必须有

$$\alpha^j \not\equiv 1 \pmod{M} \quad (j=1,\ 2,\ \cdots,\ N-1),$$

否则, 如对某个 $j(1\leqslant j\leqslant N-1)$, 有 $\alpha^j\equiv 1(\mathrm{mod}M)$, 那么由(3),就有 $N\equiv 0(\mathrm{mod}M)$, 但这与 $(N,\ M)=1$ 矛盾. 另外,在(3)中取 $j=1$, 在(3)式两端乘以 $\alpha-1(\neq 0)$, 得

$$\alpha^N\equiv 1(\mathrm{mod}M).$$

这表示 α 对模 M 为 N 阶本原单位根.

由于(3)式成立,显然有

$$\sum_{n=0}^{N-1}\alpha^{nj}\equiv 0 \pmod{p_i} \quad (j=1,\ 2,\ \cdots,\ N-1),$$

同样必须有 $\alpha^j\not\equiv 1 \ (\mathrm{mod}p_i)\ (j=1,\ 2,\ \cdots,\ N-1)$, 否则将得到 $N\equiv 0(\mathrm{mod}p_i)$,这与 $(N,\ M)=1$ 矛盾. 再在上式中取 $j=1$, 并在两端乘以 $\alpha-1$, 就可得到 $\alpha^N\equiv 1(\mathrm{mod}p_i)$. 这正表示 α 对模 $p_i(i=1,\ 2,\ \cdots,\ s)$ 的阶数为 N. 此即必要性.

再证充分性.

由于 α 是对模 $p_i(i=1,\ 2,\ \cdots,\ s)$ 的 N 次本原单位根,故

$$p_i\nmid\alpha^j-1 \quad (j=1,\ 2,\ \cdots,\ N-1;\ \ i=1,\ 2,\ \cdots,\ s).$$

由于 p_i 是素数, 所以 $(p_i,\ \alpha^j-1)=1\ (j=1,\ 2,\ \cdots,\ N-1;\ i=1,\ 2,\ \cdots,\ s)$. 又由于

$$(\alpha^j-1)\sum_{n=0}^{N-1}\alpha^{nj}\equiv\alpha^{jN}-1\equiv 0 \pmod{p_i},$$

故有

$$\sum_{n=0}^{N-1}\alpha^{nj}\equiv 0(\mathrm{mod}p_i)$$

$$(j=1,\ 2,\ \cdots,\ N-1;\ i=1,\ 2,\ \cdots,\ s).$$

因为 $(p_i,\ \alpha^j-1)=1$, 故 $(p_i^{l_i},\ \alpha^j-1)=1\ (j=1,\ 2,\ \cdots,\ N-1;\ i=1,\ 2,\ \cdots,\ s)$, 又由于

$$\alpha^j-1\not\equiv 0(\mathrm{mod}M) \quad (j=1,\ 2,\ \cdots,\ N-1),$$

所以有

$$(M,\ \alpha^j-1)=1 \quad (j=1,\ 2,\ \cdots,\ N-1).$$

而 $$(\alpha^{j}-1)\sum_{n=0}^{N-1}\alpha^{nj}\equiv\alpha^{jN}-1\equiv 0\ (\mathrm{mod} M)$$
$$(j=1,\ 2,\ \cdots,\ N-1),$$

从而有 $$\sum_{n=0}^{N-1}\alpha^{nj}\equiv 0\ (\mathrm{mod} M)\quad (j=1,\ 2,\ \cdots,\ N-1).$$

再由N^{-1}存在以及$\alpha^{N}\equiv 1(\mathrm{mod} M)$,故(1)与(2)为一对可逆变换.

定理证毕.

定理 1 中的条件 2° 与 3° 不能放宽为只剩下 2°. 如果只剩 2°, (1)与(2)就可能不是一对互逆变换. 例如

$$M=15=3\cdot 5,\quad \alpha=2,\quad N=4.$$

显然，在 Z_{15} 中，4 具有逆元 4, $\alpha=2$ 对模 15 是 4 阶单位根，但变换矩阵 T 为:

$$T\equiv\begin{bmatrix}1&1&1&1\\1&2&4&8\\1&4&1&4\\1&8&4&2\end{bmatrix}(\mathrm{mod}15),$$

T 是不可逆的（$|T|\equiv 3(\mathrm{mod}15)$, 3 与 15 不互素，故在 Z_{15} 中，3 的逆元不存在）. 这是因为 2 对模 3 不是 4 阶本原单位根，而只是 2 阶单位根，不满足定理 1 的条件 3° 的缘故. 换句话说，取参数 $M=15$, $N=4$, $\alpha=2$ 不能构成可逆的数论变换，也就是说，不能使

$$\sum_{n=0}^{3}2^{nj}\equiv 0\quad (j=1,\ 2,\ 3)\ (\mathrm{mod}15).$$

例如，取 $j=2$, 就有

$$\sum_{n=0}^{3}2^{2n}=1+2^2+2^4+2^6\equiv 1+4+1+4\equiv 10\not\equiv 0(\mathrm{mod}15).$$

因此，定理 1 的条件是缺一不可的.

定理 2 设 $M=p_1^{l_1}\cdot p_2^{l_2}\cdots p_s^{l_s}$, 当且仅当

1° N^{-1}在Z_M上存在，即$(N, M)=1$；

2° α对模$p_i^{l_i}$ $(i=1, 2, \cdots, s)$ 是 N 阶本原单位根，则(1)与(2)为一对互逆变换。

证明 由于α对模$p_i^{l_i}(i=1, 2, \cdots, s)$的阶数为$N$，故由3 五 中的7°，$\alpha$对模$M$的阶也是$N$。其次还可证明，$\alpha$对模$p_i(i=1, 2, \cdots, s)$ 的阶也是N。如若不然，设存在一个$j(1\leqslant j\leqslant N-1)$及某个$p_i$，使

$$p_i|\alpha^j-1.$$

那么，由于

$$(\alpha^j-1)\sum_{n=0}^{N-1}\alpha^{nj}\equiv\alpha^{Nj}-1\equiv0(\bmod p_i^{l_i}), \tag{**}$$

可得
$$(\alpha^j-1)\sum_{n=0}^{N-1}\alpha^{nj}\equiv0(\bmod p_i).$$

由于假设N^{-1}在Z_M上存在，即$(N, M)=1$，这时必有

$$\sum_{n=0}^{N-1}\alpha^{nj}\not\equiv0\ (\bmod p_i).$$

否则，将$\alpha^j\equiv1(\bmod p_i)$代入

$$\sum_{n=0}^{N-1}\alpha^{nj}\equiv0\ (\bmod p_i),$$

就得$N\equiv0(\bmod p_i)$，这与$(N, M)=1$的假设矛盾。由于p_i为素数，所以$\left(p_i, \sum_{n=0}^{N-1}\alpha^{nj}\right)=1$，从而有

$$\left(p_i^{l_i}, \sum_{n=0}^{N-1}\alpha^{nj}\right)=1.$$

因此，由上面(**)式，便有$\alpha^j-1\equiv0(\bmod p_i^{l_i})$。但这与$N$是$\alpha$对模$p_i^{l_i}$的阶数矛盾。故

$$p_i\nmid\alpha^j-1\quad(j=1, 2, \cdots, N-1;\ i=1, 2, \cdots, s).$$

又由于
$$\alpha^N\equiv1(\bmod p_i)\quad(i=1, 2, \cdots, s),$$

所以α对模$p_i(i=1, 2, \cdots, s)$的阶为N。再由N^{-1}在Z_M上

存在，故由定理1知，(1)与(2)为一对互逆变换.

以上即定理的充分性. 至于必要性，基本上和定理1的证明类似. 事实上，由于(1)和(2)是一对互逆变换，由定理1知，N^{-1} 在 Z_M 上存在，α 不但对模 M 是 N 阶本原单位根，同时对模 $p_i(i=1, 2, \cdots, s)$ 也是 N 阶本原单位根. 由于

$$(p_i^{l_i}, \alpha^j-1)=(p_i, \alpha^j-1)=1$$
$$(j=1, 2, \cdots, N-1; i=1, 2, \cdots, s),$$

也就是说，当 $p_i \nmid \alpha^j-1$ 时，$p_i^{l_i} \nmid \alpha^j-1$ $(j=1, 2, \cdots, N-1; i=1, 2, \cdots, s)$，又由于 $M|\alpha^N-1$，故 $p_i^{l_i}|\alpha^N-1$. 这就表示 α 是模 $p_i^{l_i}$ 的 N 阶本原单位根. 定理证毕.

推论 在定理2的条件下，有

$$(\alpha^j-1, p_i^{l_i})=1 \quad (j=1, 2, \cdots, N-1; i=1, 2, \cdots, s).$$
$$(\alpha^j-1, M)=1 \quad (j=1, 2, \cdots, N-1).$$

在一般情况下，α 如对模 $p_i^{l_i}$ 的阶为 m，m 与 M 不互素，那么就不一定有$(\alpha^j-1, p_i^{l_i})=1(j=1, 2, \cdots, m-1)$. 例如，$M=p^l=3^2=9$，$\alpha=2$ 对模9是6阶单位根，但$(2^2-1, 9)\neq1$. 这是因为$(6, 9)=3\neq1$ 的缘故.

在定理1的证明中，关键是

$$(\alpha^j-1, M)=1(j=1, 2, \cdots, N-1). \tag{4}$$

(4)式意味着，在 Z_M 上存在 $\beta_j(j=1, 2, \cdots, N-1)$，使

$$\beta_j(\alpha^j-1)\equiv1(\mathrm{mod}M)\ (j=1, 2, \cdots, N-1).$$

因此有

定理3 设 M 为任一自然数，当且仅当

1° N^{-1} 在 Z_M 上存在，即$(N, M)=1$;

2° α 对模 M 是 N 阶本原单位根;

3° 在 Z_M 上存在 $\beta_j(j=1, 2, \cdots, N-1)$，使

$$\beta_j(\alpha^j-1)\equiv1(\mathrm{mod}M) \quad (j=1, 2, \cdots, N-1) \tag{5}$$

时，(1)与(2)为一对互逆变换．当 M 为素数时，条件 2° 包含条件 3°．

证明 欲使(2)存在，N^{-1} 必需在 Z_M 上存在．而

$$\sum_{n=0}^{N-1}\alpha^{nj}\equiv\beta_j(\alpha^j-1)\sum_{n=0}^{N-1}\alpha^{nj}\equiv\beta_j(\alpha^{jN}-1)$$

$$\equiv 0(\mathrm{mod}M)\quad(j=1,\ 2,\ \cdots,\ N-1).$$

此即充分性*．

反之，当

$$\sum_{n=0}^{N-1}\alpha^{nj}\equiv 0(\mathrm{mod}M)\quad(j=1,\ 2,\ \cdots,\ N-1)$$

时，有 $\alpha^N-1=(\alpha-1)\sum\limits_{n=0}^{N-1}\alpha^n\equiv 0\ (\mathrm{mod}M)$，同时必有 $\alpha^j\not\equiv 1\ (\mathrm{mod}M)\ (j=1,\ 2,\ \cdots,\ N-1)$．否则将与 N^{-1} 在 Z_M 上存在矛盾．这表示 α 对模 M 是 N 阶单位根．

又设 p 为 M 的任一素因子，用定理 1 的证法，可以证明 α 对模 p 的阶数为 N，故 $(p,\ \alpha^j-1)=1(j=1,\ 2,\cdots,\ N-1)$，于是 $(M,\ \alpha^j-1)=1(j=1,\ 2,\ \cdots,\ N-1)$．这样，$\alpha^j-1$ 在 Z_M 上存在逆元，记为 β_j，从而有

$$\beta_j(\alpha^j-1)\equiv 1(\mathrm{mod}M)\quad(j=1,\ 2,\ \cdots,\ N-1).$$

此即必要性．定理 3 证毕．

定理 4 设 $M=p_1^{l_1}\cdot p_2^{l_2}\cdots p_s^{l_s}$，当且仅当

$$N\,|\,O(M)=(p_1-1,\ p_2-1,\ \cdots,\ p_s-1)\tag{6}$$

时，(1)与(2)成为一对互逆变换．其中

$$O(M)=(p_1-1,\ p_2-1,\ \cdots,\ p_s-1)$$

表示 $p_1-1,\ p_2-1,\ \cdots,\ p_s-1$ 的最大公约数．

---

* 在充分性的证明中，似乎只用到 α 是 Z_M 上的 N 次单位根，而没有用到是对模 M 的 N 阶单位根．但这是必要的，如果对某个 $j(1\leqslant j\leqslant N-1)$，有 $\alpha^j\equiv 1\ (\mathrm{mod}M)$．则可得到 $N\equiv 0(\mathrm{mod}M)$，这与 $(N,\ M)=1$ 矛盾．

证明 如果 (1) 与 (2) 为 Z_M 上的一对互逆变换，那么由定理 1，α 对模 p_i 的阶为 N，故由 Fermat 定理知

$$N \mid \varphi(p_i) = p_i - 1 (i=1, 2, \cdots, s),$$

这表示 N 是 $p_1-1, p_2-1, \cdots, p_s-1$ 的公约数，所以有

$$N \mid O(M) = (p_1-1, p_2-1, \cdots, p_s-1).$$

此即必要性.

反之，如果 $N \mid O(M)$，即 $N \mid p_i - 1 (i=1, 2, \cdots, N-1)$. 这表示 N 与 p_i 互素，从而 N 与 $p_i^{l_i}$ 互素，所以 N 与 M 互素，即 $(N, M)=1$，所以 N^{-1} 在 Z_M 中存在.

其次，由 **3** 五 之 8°，当模为 $p_i^{l_i}$ 时，有主根存在，记为 g_i，即

$$g_i^{\varphi(p_i^{l_i})} \equiv 1 (\bmod p_i^{l_i}) \quad (i=1, 2, \cdots, s).$$

记
$$\alpha_i = g_i^{\frac{\varphi(p_i^{l_i})}{N}} \quad (i=1, 2, \cdots, s),$$

那么，α_i 对模 $p_i^{l_i}$ 的阶数为 N. 也就是说，存在对模 $p_i^{l_i}$ 的阶数为 N 的本原单位根 α_i，

$$\alpha_i^N \equiv 1 (\bmod p_i^{l_i}) \quad (i=1, 2, \cdots, s).$$

由孙子定理，可求出如下同余方程组的解：

$$\alpha \equiv \alpha_i (\bmod p_i^{l_i}) \quad (i=1, 2, \cdots, s).$$

其解可写作
$$\alpha \equiv \sum_{i=1}^{s} M_i' M_i \alpha_i (\bmod M),$$

其中
$$M_i' M_i \equiv 1 (\bmod p_i^{l_i}) \quad (i=1, 2, \cdots, s).$$

由于 α_i 对模 $p_i^{l_i}$ 的阶数为 N，故 α 对模 $p_i^{l_i}$ 的阶数也为 N. 于是，由定理 2 知，这样求出的 α 与 M、N 一起便给出 Z_M 上的一对互逆变换 (1) 与 (2).

定理 4 证毕.

定理 5　在定理 1~4 的条件下，变换(1)与(2)具有循环卷积特性.

定理 5 的证明完全与 **2** 中定理 1 相同.

推论　在以正整数 M 为模的整数环 Z_M 上，具有循环卷积特性的变换的最大长度是

$$N_{\max}=O(M).$$

定理 4 极为重要，它使我们能对给定的正整数 M 具体选取变换长度 N，从而确定 α，以构成数论变换. 关于 M, N, α 的具体选择，将在 **6** 及 **7** 中详细讨论.

总结起来说，本节讨论了在 Z_M 上 NTT 的存在条件，从上述定理所述条件的充分必要性及其证明，我们实际上得到如下的结论:

设 $M=p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s}$, $N\in Z_M$, $\alpha\in Z_M$, 则下述诸命题互相等价:

1° (1)与(2)是一对可逆变换;

2° $(N, M)=1$, $(\alpha, M)=1$,

$$N^{-1}\sum_{n=0}^{N-1}\alpha^{nj}\equiv\begin{cases}1, & j\equiv 0(\bmod N)\\ 0, & j\not\equiv 0(\bmod N)\end{cases}(\bmod M);$$

3° $(N, M)=1$, α 是模 M 的 N 阶本原单位根，α 是模 p_i 的 N 阶本原单位根$(i=1, 2, \cdots, s)$;

4° $(N, M)=1$, α 是模 $p_i^{l_i}(i=1, 2, \cdots, s)$ 的 N 阶本原单位根;

5° $(N, M)=1$, α 是模 M 的 N 阶本原单位根，且

$$(\alpha^j-1, M)=1 \quad (j=1, 2, \cdots, N-1);$$

6° $(N, M)=1$, α 是模 M 的 N 阶本原单位根，且在 Z_M 上存在 β_j, 使 $\beta_j(\alpha^j-1)\equiv 1(\bmod M)$ $(j=1, 2, \cdots, N-1)$;

7° $N|O(M)$.

从上述命题可知，α 仅是模 M 的 N 阶本原单位根还不够，必需再加上某个适当的条件，才能使(1)和(2)构成一对互逆变换. 命题 C, D 是今后由 M, N 计算 α 的基础，由命题 G 证明命题 A 的方法(即定理 4 的充分性)是由 M, N 计算 α 的具体步骤，命题 E 和 F 使我们有可能讨论复数数论变换，而其中 α 是模 M 的 N 阶本原单位根仅是必要条件.

—5—

例、数论变换的性质

首先，通过具体的例子，说明数论变换的构造。

一、几种典型序列的数论变换

(一)δ-函数序列的变换

对 $\delta(t)$ 函数进行采样，得到序列

$$(x)=\{x_n\}=\begin{bmatrix}1\\0\\0\\0\end{bmatrix}$$

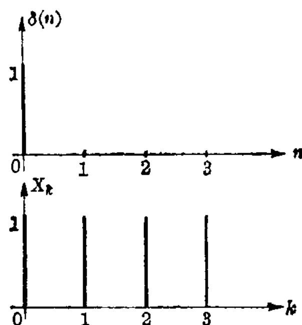


图 1

取 NTT 的参数为 $M=17$，$N=4$，$\alpha=4$，由 **4** 中定理 1 可以证明，以这些参数可以构成数论变换。这时变换矩阵 T_4 为：

$$T_4 \equiv \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 4 & 4^2 & 4^3 \\ 1 & 4^2 & 4^4 & 4^6 \\ 1 & 4^3 & 4^6 & 4^9 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 4 & -1 & -4 \\ 1 & -1 & 1 & -1 \\ 1 & -4 & -1 & 4 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 4 & 16 & 13 \\ 1 & 16 & 1 & 16 \\ 1 & 13 & 16 & 4 \end{bmatrix} (\mathrm{mod}17).$$

所以

$$(X) = \begin{bmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \end{bmatrix} \equiv T_4 \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 4 & 16 & 13 \\ 1 & 16 & 1 & 16 \\ 1 & 13 & 16 & 4 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} (\mathrm{mod}17).$$

x_n 和 X_k 表示于图 1 中，和 δ-函数序列的 DFT 一样，其数论变换序列(或可称为像序列或谱序列)是常数.

(二)一个恒定值的采样序列的变换

设一序列(x)为

$$(x) = \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{N-1} \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix},$$

取定 NTT 的参数 M, N, α, 则

$$(X)=\begin{bmatrix} X_0 \\ X_1 \\ X_2 \\ \vdots \\ X_{N-1} \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha & \cdots & \alpha^{N-1} \\ 1 & \alpha^2 & \cdots & \alpha^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{N-1} & \cdots & \alpha^{(N-1)^2} \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$$

$$\equiv \begin{bmatrix} N \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} (\mathrm{mod} M).$$

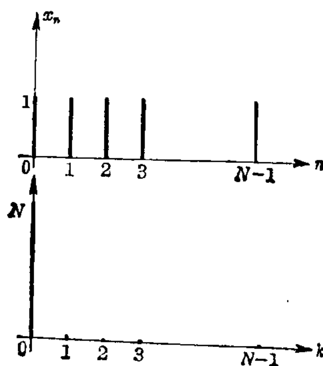


图 2

x_n 与 X_k 表示在图 2 中.

(三)正弦波序列的变换

对正弦波 $x(t)=\sin wt$ 的一个周期进行采样，所得的序列为:

$$(x)=\begin{bmatrix}x_0\\x_1\\x_2\\x_3\end{bmatrix}=\begin{bmatrix}0\\1\\0\\-1\end{bmatrix}.$$

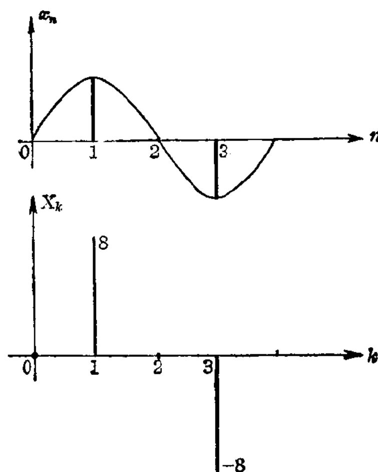


图 3

取 NTT 的参数为 $M=17$, $N=4$, $\alpha=4$, 变换矩阵 T_4 如例 1 所示, 则

$$(X)=\begin{bmatrix}X_0\\X_1\\X_2\\X_3\end{bmatrix}\equiv T_4\begin{bmatrix}0\\1\\0\\-1\end{bmatrix}\equiv\begin{bmatrix}1&1&1&1\\1&4&16&13\\1&16&1&16\\1&13&16&4\end{bmatrix}\begin{bmatrix}0\\1\\0\\-1\end{bmatrix}$$

$$\equiv\begin{bmatrix}0\\-9\\0\\9\end{bmatrix}\equiv\begin{bmatrix}0\\8\\0\\-8\end{bmatrix}(\bmod 17).$$

x_n 和 X_k 表示在图 3 中. 变换结果 X_k 在 $\left[-\frac{M}{2}, \frac{M}{2}\right]$ 中取值，其理由见 **6**.

二、数论变换的性质

NTT 基本上和 DFT 一样，具有如下性质.

(一)线性

如果 $T\{x_n\}=X_k$, $T\{y_n\}=Y_k$, 那么

$$T\{ax_n+by_n\}=aT\{x_n\}+bT\{y_n\}=aX_k+bY_k, \qquad (1)$$

其中 a、b 为常数. T 表示 NTT.

(二)正交性

记变换 T 的行矢量为 $\{\varphi_i(n)\}$, 称 $\{\varphi_i(n)\}$ 为基函数. 即

$$\{\varphi_0(n)\}=(1, 1, 1, \cdots, 1),$$

$$\{\varphi_1(n)\}=(1, \alpha, \alpha^2, \cdots, \alpha^{N-1}),$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\{\varphi_i(n)\}=(1, \alpha^i, \alpha^{2i}, \cdots, \alpha^{i(N-1)}),$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\{\varphi_{N-1}(n)\}=(1, \alpha^{N-1}, \alpha^{2(N-1)}, \cdots, \alpha^{(N-1)^2}).$$

基函数内积的定义是

$$\langle\varphi_i(n), \varphi_k(n)\rangle\equiv\sum_{n=0}^{N-1}\varphi_i(n)\varphi_k^{-1}(n) \quad (\bmod M).$$

于是有

$$\langle\varphi_i(n), \varphi_k(n)\rangle\equiv\sum_{n=0}^{N-1}\alpha^{ni}\cdot\alpha^{-nk}\equiv\sum_{n=0}^{N-1}\alpha^{n(i-k)}$$

$$\equiv\begin{cases}N, & i\equiv k \ (\bmod N)\\ 0, & i\not\equiv k \ (\bmod N)\end{cases}(\bmod M). \qquad (2)$$

这表示 NTT 是一种正交变换.

（三）周期性

设 $T\{x_n\}=X_k$, $T^{-1}\{X_k\}=x_n$, 那么有

$$x_{n+SN}\equiv x_n(\bmod M),\qquad X_{k+SN}\equiv X_k(\bmod M),\tag{3}$$

其中，S 为整数，n, $k=0, 1, \cdots, N-1$. 这表示 x_n 和 X_k 均为以 N 为周期的周期序列.

证明 由 NTT 的定义可知，有

$$X_{k+SN}\equiv\sum_{n=0}^{N-1}x_n\alpha^{n(k+SN)}\equiv\sum_{n=0}^{N-1}x_n\alpha^{nk}\alpha^{nSN}$$

$$\equiv\sum_{n=0}^{N-1}x_n\alpha^{nk}\equiv X_k(\bmod M)\qquad(k=1,\cdots,N-1).$$

同理可证 $x_{n+SN}\equiv x_n(\bmod M)$.

另外，利用 $\alpha^N\equiv1(\bmod M)$ 及 x_n 和 X_k 的周期性，可以证明

$$\left.\begin{aligned}&\sum_{n=p}^{q}x_n\alpha^{nk}\equiv\sum_{n=0}^{N-1}x_n\alpha^{nk}&&(\bmod M),\\&N^{-1}\sum_{k=p}^{q}X_k\alpha^{-nk}\equiv N^{-1}\sum_{k=0}^{N-1}X_k\alpha^{-nk}&&(\bmod M),\end{aligned}\right\}\tag{4}$$

其中 $|q-p|=N-1$.

为了证明(4)式，不妨设 $p=SN+r(0\leqslant r<N-1$, S 为整数), $q=p+N-1$. 于是

$$\sum_{n=p}^{q}x_n\alpha^{nk}=\sum_{n=SN+r}^{SN+r+N-1}x_n\alpha^{nk}\equiv\sum_{l=r}^{r+N-1}x_l\alpha^{lk}$$

$$=\sum_{l=r}^{N-1}x_l\alpha^{lk}+\sum_{l=N}^{r+N-1}x_l\alpha^{lk}=\sum_{l=r}^{N-1}x_l\alpha^{lk}+\sum_{l=0}^{r-1}x_l\alpha^{lk}$$

$$=\sum_{l=0}^{N-1}x_l\alpha^{lk}\quad(\bmod M).$$

同理可证(4)式的另一式.

（四）**对称性***

如果序列 x_n 是对称的，即 $x_n=x_{-n}=x_{N-n}$，那么其象序列也是对称的，即

$$X_k\equiv X_{-k}\equiv X_{N-k}(\bmod M)\quad (k=0,\ 1,\ \cdots,\ N-1).\quad (5)$$

如果序列 x_n 是反对称的，即 $x_n=-x_{-n}=-x_{N-n}$，那么其象序列也是反对称的，即

$$X_k\equiv -X_{-k}\equiv -X_{N-k}(\bmod M)\quad (k=0,\ 1,\ \cdots,\ N-1).\quad (6)$$

证明

$$X_{-k}\equiv\sum_{n=0}^{N-1}x_n\alpha^{-nk}=\sum_{l=0}^{-N+1}x_{-l}\alpha^{lk}=\sum_{l=0}^{N-1}x_{-l}\alpha^{lk}$$

$$=\begin{cases}\sum\limits_{l=0}^{N-1}x_l\alpha^{lk}\equiv X_k, & 如果\ x_{-l}=x_l,\\ -\sum\limits_{l=0}^{N-1}x_l\alpha^{lk}\equiv -X_k, & 如果\ x_{-l}=-x_l,\end{cases}(\bmod M).$$

对称性可叙述作：偶序列的象序列为偶序列，奇序列的象序列为奇序列.

（五）**位移定理**

设 $T\{x_n\}=X_k$，则

$$T\{x_{n+m}\}\equiv X_k\alpha^{-mk}(\bmod M),\quad (7)$$

其中，m 为任意整数，$k=0,\ 1,\ \cdots,\ N-1$.

证明 $T\{x_{n+m}\}\equiv\sum\limits_{n=0}^{N-1}x_{n+m}\alpha^{nk}=\sum\limits_{l=m}^{m+N-1}x_l\alpha^{k(l-m)}$

$$=\alpha^{-mk}\sum_{l=0}^{N-1}x_l\alpha^{kl}\equiv X_k\alpha^{-mk}(\bmod M).$$

（六）**循环卷积特性**

设两个长为 N 的序列 x_n 和 h_n，其循环卷积记为 y_n，即

$$y_n=\sum_{k=0}^{N-1}x_k h_{\langle n-k\rangle_N}\quad (n=0,\ 1,\ \cdots,\ N-1).$$

---

* 这里及以后均指周期序列.

如果记 $\{X_k\}=T\{x_n\}$, $\{H_k\}=T\{h_n\}$, $\{Y_k\}=T\{y_n\}$, 则

$$Y_k \equiv X_k \cdot H_k (\bmod M) \quad (k=0,\ 1,\ \cdots,\ N-1). \tag{8}$$

此特性在 **2** 中已经证明.

(七)相关特性

设两个以 N 为周期的周期序列 x_n 和 h_n, 称

$$y_n=\sum_{m=0}^{N-1} x_m h_{n+m} \quad (n=0,\ 1,\ \cdots,\ N-1)$$

为序列 x_n 和 h_n 的互相关序列. 如果 x_n 和 h_n 相等, 则称为自相关序列.

设 $\quad X_k=T\{x_n\},\quad H_k=T\{h_n\},\quad Y_k=T\{y_n\}$,

则

$$Y_k \equiv X_{-k} \cdot H_k \equiv X_{N-k} \cdot H_k (\bmod M) \quad (k=0,1,\cdots,N-1). \tag{9}$$

证明

$$Y_k \equiv T\{y_n\}=\sum_{n=0}^{N-1} y_n \alpha^{nk}=\sum_{n=0}^{N-1}\left[\sum_{m=0}^{N-1} x_m h_{n+m}\right]\alpha^{nk}$$

$$=\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} x_m h_{n+m}\alpha^{nk}=\sum_{m=0}^{N-1} x_m\left[\sum_{n=0}^{N-1} h_{n+m}\alpha^{nk}\right]$$

利用位移定理, 有

$$Y_k \equiv \sum_{m=0}^{N-1} x_m H_k \alpha^{-mk} \equiv H_k X_{-k} \equiv H_k X_{N-k} (\bmod M).$$

(八)Parseval 定理

设 $X_k=T\{x_n\}$, $H_k=T\{h_n\}$, 则

$$N\sum_{n=0}^{N-1} x_n h_n \equiv \sum_{k=0}^{N-1} X_k H_{-k}=\sum_{k=0}^{N-1} X_k H_{N-k} (\bmod M), \tag{10}$$

$$N\sum_{n=0}^{N-1} x_n h_{-n}=N\sum_{n=0}^{N-1} x_n h_{N-n} \equiv \sum_{k=0}^{N-1} X_k H_k (\bmod M). \tag{11}$$

特别当 $x_n=h_n$ $(n=0,\ 1,\ \cdots,\ N-1)$时, 有

$$N\sum_{n=0}^{N-1} x_n^2 \equiv \sum_{k=0}^{N-1} X_k \cdot X_{-k}=\sum_{k=0}^{N-1} X_k \cdot X_{N-k} (\bmod M), \tag{10'}$$

$$N\sum_{n=0}^{N-1} x_n \cdot x_{-n} = N\sum_{n=0}^{N-1} x_n \cdot x_{N-n} \equiv \sum_{k=0}^{N-1} X_k^2 (\bmod M). \qquad (11')$$

证明 证明(10)式. (11)式的证法相同.

$$\sum_{k=0}^{N-1} X_k \cdot H_{-k} \equiv \sum_{k=0}^{N-1} \left[\sum_{n=0}^{N-1} x_n \alpha^{nk}\right]\left[\sum_{m=0}^{N-1} h_m \alpha^{-mk}\right]$$

$$= \sum_{n=0}^{N-1} x_n \sum_{m=0}^{N-1} h_m \sum_{k=0}^{N-1} \alpha^{k(n-m)} \quad (\bmod M),$$

由于

$$\sum_{k=0}^{N-1} \alpha^{k(n-m)} \equiv \begin{cases} N, & n \equiv m \quad (\bmod N) \\ 0, & n \not\equiv m \quad (\bmod N) \end{cases} \quad (\bmod M).$$

故

$$\sum_{k=0}^{N-1} X_k H_{-k} \equiv N \sum_{n=0}^{N-1} x_n h_n \quad (\bmod M).$$

在复数域中，DFT 的 Parseval 等式为

$$N\sum_{n=0}^{N-1} |x_n|^2 = \sum_{k=0}^{N-1} |X_k|^2.$$

在现在的情况下，上式不再有意义，因为在 Z_M 上，模值 $|X_n|^2$ 不再有定义.

(九)快速算法

在复数域中，当 N 是高度复合数时，特别当 $N=2^m$ 时，DFT 有快速算法(FFT). NTT 也有快速算法($N=2^m$). 其推导和演算完全和 FFT 相同. 但不同之处有两点，第一是以 α 代替 FFT 中的 W_N，由于 α 是一正整数，不像 FFT 那样要预先贮存基函数 W_N；第二是每一步运算过程都要判别一下中间量是否超过 M，如果超过 M，就应取小于 M 的同余值，以防溢出.

下面以矩阵表示法，简要地推导快速算法.

设变换参数为 $M, N=8$, α; $x_n \in Z_M (n=0, 1, \cdots, N-1)$，于是

$$\begin{bmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \\ X_5 \\ X_6 \\ X_7 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} & \alpha^{21} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha^{16} & \alpha^{20} & \alpha^{24} & \alpha^{28} \\ 1 & \alpha^5 & \alpha^{10} & \alpha^{15} & \alpha^{20} & \alpha^{25} & \alpha^{30} & \alpha^{35} \\ 1 & \alpha^6 & \alpha^{12} & \alpha^{18} & \alpha^{24} & \alpha^{30} & \alpha^{36} & \alpha^{42} \\ 1 & \alpha^7 & \alpha^{14} & \alpha^{21} & \alpha^{28} & \alpha^{35} & \alpha^{42} & \alpha^{49} \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & 1 & \alpha^2 & \alpha^4 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha & \alpha^4 & \alpha^7 & \alpha^2 & \alpha^5 \\ 1 & \alpha^4 & 1 & \alpha^4 & 1 & \alpha^4 & 1 & \alpha^4 \\ 1 & \alpha^5 & \alpha^2 & \alpha^7 & \alpha^4 & \alpha & \alpha^6 & \alpha^3 \\ 1 & \alpha^6 & \alpha^4 & \alpha^2 & 1 & \alpha^6 & \alpha^4 & \alpha^2 \\ 1 & \alpha^7 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} (\bmod M)。$$

按如下次序交换矩阵的行

$$\begin{bmatrix} X_0 \\ X_4 \\ X_2 \\ X_6 \\ X_1 \\ X_5 \\ X_3 \\ X_7 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha^4 & 1 & \alpha^4 & 1 & \alpha^4 & 1 & \alpha^4 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & 1 & \alpha^2 & \alpha^4 & \alpha^6 \\ 1 & \alpha^6 & \alpha^4 & \alpha^2 & 1 & \alpha^6 & \alpha^4 & \alpha^2 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^5 & \alpha^2 & \alpha^7 & \alpha^4 & \alpha & \alpha^6 & \alpha^3 \\ 1 & \alpha^3 & \alpha^6 & \alpha & \alpha^4 & \alpha^7 & \alpha^2 & \alpha^5 \\ 1 & \alpha^7 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} (\bmod M),$$

如果注意到： $\alpha^8 \equiv 1 (\bmod M)$.

$$\alpha^4 \equiv -1 (\mathrm{mod} M).$$

上述变换矩阵 T 就成为

$$T=\begin{bmatrix}1&1&1&1&1&1&1&1\\1&-1&1&-1&1&-1&1&-1\\1&\alpha^2&-1&-\alpha^2&1&\alpha^2&-1&-\alpha^2\\1&-\alpha^2&-1&\alpha^2&1&-\alpha^2&-1&\alpha^2\\1&\alpha&\alpha^2&\alpha^3&-1&-\alpha&-\alpha^2&-\alpha^3\\1&-\alpha&\alpha^2&-\alpha^3&-1&\alpha&-\alpha^2&\alpha^3\\1&\alpha^3&-\alpha^2&\alpha&-1&-\alpha^3&\alpha^2&-\alpha\\1&-\alpha^3&-\alpha^2&-\alpha&-1&\alpha^3&\alpha^2&\alpha\end{bmatrix}.$$

这个矩阵左上角与右上角子矩阵相同，左下角与右下角子矩阵只相差一个-1. 故可将 T 分解为如下两个矩阵之乘积:

$$T=\left[\begin{array}{cccc|cccc}1&1&1&1&&&&\\1&-1&1&-1&&&0&\\1&\alpha^2&-1&-\alpha^2&&&&\\1&-\alpha^2&-1&\alpha^2&&&&\\\hline&&&&1&1&1&1\\&&0&&1&-1&1&-1\\&&&&1&\alpha^2&-1&-\alpha^2\\&&&&1&-\alpha^2&-1&\alpha^2\end{array}\right]\cdot\left[\begin{array}{cccc|cccc}1&&&&1&&&\\&1&&&&1&&\\&&1&&&&1&\\&&&1&&&&1\\\hline1&&&&-1&&&\\&\alpha&&&&-\alpha&&\\&&\alpha^2&&&&-\alpha^2&\\&&&\alpha^3&&&&-\alpha^3\end{array}\right].$$

又由于

$$
\begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 \\
1 & \alpha^2 & -1 & -\alpha^2 \\
1 & -\alpha^2 & -1 & \alpha^2
\end{bmatrix}
=
\begin{bmatrix}
1 & 1 & 0 & 0 \\
1 & -1 & 0 & 0 \\
0 & 0 & 1 & 1 \\
0 & 0 & 1 & -1
\end{bmatrix}
\cdot
\begin{bmatrix}
1 & & 1 & \\
 & 1 & & 1 \\
1 & & -1 & \\
 & \alpha^2 & & -\alpha^2
\end{bmatrix},
$$

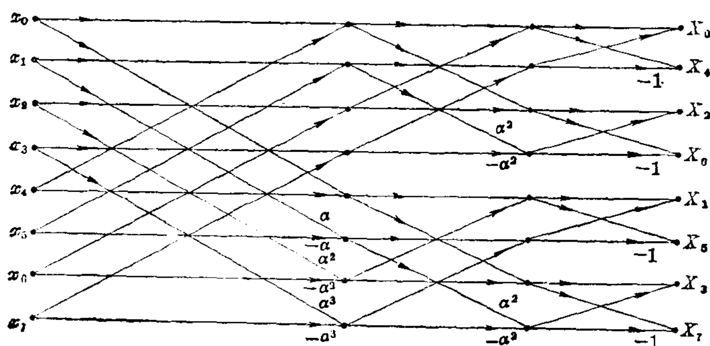
因此有

$$
\begin{bmatrix}
X_0 \\ X_4 \\ X_2 \\ X_6 \\ X_1 \\ X_5 \\ X_3 \\ X_7
\end{bmatrix}
\equiv
\left[\begin{array}{cccc|cccc}
1 & 1 & & & & & & \\
1 & -1 & & & & & & \\
 & & 1 & 1 & & & & \\
 & & 1 & -1 & & & & \\
\hline
 & & & & 1 & 1 & & \\
 & & & & 1 & -1 & & \\
 & & & & & & 1 & 1 \\
 & & & & & & 1 & -1
\end{array}\right]
$$

$$
\cdot
\left[\begin{array}{cccc|cccc}
1 & & 1 & & & & & \\
 & 1 & & 1 & & & & \\
1 & & -1 & & & & & \\
 & \alpha^2 & & -\alpha^2 & & & & \\
\hline
 & & & & 1 & & 1 & \\
 & & & & & 1 & & 1 \\
 & & & & 1 & & -1 & \\
 & & & & & \alpha^2 & & -\alpha^2
\end{array}\right]
$$

$$
\cdot\begin{bmatrix}
1 & & & & 1 & & & \\
& 1 & & & & 1 & & \\
& & 1 & & & & 1 & \\
& & & 1 & & & & 1 \\
1 & & & & -1 & & & \\
& \alpha & & & & -\alpha & & \\
& & \alpha^2 & & & & -\alpha^2 & \\
& & & \alpha^3 & & & & -\alpha^3
\end{bmatrix}\cdot\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix},
$$

由上式，得到快速算法的流程图如下：



其中 $x_n \xrightarrow{\alpha^i} y$，$x_m \xrightarrow{\alpha^j} y$ 或 $x_n \xrightarrow{\alpha^i} y$，$x_m \xrightarrow{\alpha^j} y$

均表示 $y=x_n\alpha^i+x_m\alpha^j$. 这相当于 FFT 的按频率抽取的算法. 同样可用按时间抽取的算法，读者可参阅参考文献[1].

用上述快速算法，可将原来所需的 N^2 个乘法降为 $N\log_2 N$ 次乘法. 如果 α 是 2 或 2 的幂，就只需 $N\log_2 N$ 次移位操作. 其它的快速算法，可参阅本丛书《快速傅里叶变换》.

(十)抽样性质

这一性质研究如果将序列 x_n 按某种规律重排，其象序列按何种规律排列的问题.

设 p 和 N 互素，即 $(N, p)=1$，那么序列

$$y_n=x_{\langle pn\rangle_N} \quad (n=0, 1, \cdots, N-1) \tag{12}$$

是序列 $x_n(n=0, 1, \cdots, N-1)$ 的一个重排*. y_n 的变换为

$$Y_k \equiv T\{y_n\}=\sum_{n=0}^{N-1} y_n \alpha^{nk}=\sum_{n=0}^{N-1} x_{\langle pn\rangle_N} \alpha^{nk} (\bmod M).$$

由于 $(p, N)=1$，故 p 在 Z_N 中存在逆元 p^{-1}，并且 p^{-1} 与 N 互素，即 $(p^{-1}, N)=1$. 从而 $\langle mp^{-1}\rangle_N(m=0, 1, \cdots, N-1)$ 也是 $0, 1, 2, \cdots, N-1$ 的一个重排. 在 Y_k 的式子中作置换

$$m=\langle pn\rangle_N \quad (n=0, 1, \cdots, N-1),$$

则得到

$$Y_k \equiv \sum_{m=0}^{N-1} x_m \alpha^{\langle p^{-1}m\rangle_N k} \equiv \sum_{m=0}^{N-1} x_m \alpha^{\langle p^{-1}k\rangle_N m}$$

$$=X_{\langle kp^{-1}\rangle_N} \quad (\bmod M),$$

即

$$Y_k=X_{\langle kp^{-1}\rangle_N} \quad (k=0, 1, 2, \cdots, N-1). \tag{13}$$

此即欲证者. 等式(13)说明，如果序列的重排对应于

$$n \to \langle pn\rangle_N \quad (n=0, 1, \cdots, N-1),$$

那么，象序列的重排对应于

$$k \to \langle p^{-1}k\rangle_N \quad (k=0, 1, \cdots, N-1).$$

其中，$(p, N)=1$, $p^{-1}p\equiv 1(\bmod N)$.

例 1 取 $N=5$, $p=2$, 显然 $(2, 5)=1$, 在 Z_5 中 2 的逆元 $2^{-1}=3$. 如记 $y_n=x_{\langle 2n\rangle_5}(n=0, 1, 2, 3, 4)$，即

---

* 为了证明(12)中的 y_n 是 x_n 的一个重排，只需证明 $\langle pn\rangle_N$ $(n=0, 1, \cdots, N-1)$ 与 $0, 1, \cdots, N-1$ 一一对应即可. 由于有 $0\leqslant\langle pn\rangle_N\leqslant N-1$，故只需证明当 $n_1\neq n_2(n_1, n_2=0, 1, \cdots, N-1)$ 时，有 $pn_1\not\equiv pn_2(\bmod N)$ 即可. 这是显然的. 如果不然，存在 n_1, n_2，且 $n_1\neq n_2$，使 $pn_1\equiv pn_2(\bmod N)$，即 $N|p(n_1-n_2)$，由于 $N\nmid p$，故 $N|n_1-n_2$，又因为 $|n_1-n_2|<N$，故必有 $n_1=n_2$，但这与 $n_1\neq n_2$ 矛盾.

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} x_0 \\ x_2 \\ x_4 \\ x_1 \\ x_3 \end{bmatrix}.$$

由(13)式，得到 $Y_k = X_{\langle 3k \rangle_5}$ $(k=0, 1, 2, 3, 4)$. 即

$$\begin{bmatrix} Y_0 \\ Y_1 \\ Y_2 \\ Y_3 \\ Y_4 \end{bmatrix} = \begin{bmatrix} X_0 \\ X_3 \\ X_1 \\ X_4 \\ X_2 \end{bmatrix}.$$

特别，取 $p=N-1$，那么在 Z_N 中，$p^{-1}=N-1$. 由(12)式及(13)式，就得到

$$X_{-k} = T\{x_{-n}\}.$$

亦即

$$X_{N-k} = T\{x_{N-n}\}.$$

此即(5)式及(6)式.

(十一)延伸性质

这性质研究将长为 N 的序列 x_n 延伸成长为 rN 的序列的变换问题.

设 x_n 为长为 N 的序列，作长为 rN 的序列 y_n:

$$y_n = \begin{cases} x_n, & n=0, 1, \cdots, N-1, \\ 0, & n=N, N+1, \cdots, rN-1 \end{cases} \quad (r \text{ 为正整数}).$$

我们要研究 $Y_k = T\{y_n\}$ 与 $X_k = T\{x_n\}$ 的关系.

设 α 对模 M 的阶数为 rN，那么 α^r 对模 M 的阶数为 N. 于是

$$Y_k \equiv \sum_{n=0}^{rN-1} y_n \alpha^{nk} \equiv \sum_{n=0}^{N-1} x_n (\alpha^r)^{\frac{k}{r}n} (\bmod M)$$

$$(k=0, 1, \cdots, rN-1), \qquad (14)$$

故得到

$$Y_k \equiv \begin{cases} X_{\frac{k}{r}}, & \dfrac{k}{r}\text{为正整数时}, \\ \sum_{n=0}^{N-1} x_n \alpha^{nk}, & \text{其它}, \end{cases} \quad (\text{mod} M). \qquad (15)$$

例 2 对矩形波进行采样，得到

$$\{x_n\} = (1,\ 2,\ 1,\ 0).$$

于是

$N=4$, $\{x_n\} = (1,\ 2,\ 1,\ 0)$,

$N=8$, $\{y_n\} = (1,\ 2,\ 1,\ 0,\ 0,\ 0,\ 0,\ 0)$,

$N=16$, $\{z_n\} = (1, 2, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$.

取 NTT, 参数为 $M=17$, $N=4$, $\alpha=4$, 对 $\{x_n\}$ 进行变换，得到

$$\{X_k\} \equiv (4,\ 8,\ 0,\ -8) \quad (\text{mod} 17).$$

根据(15)式，有

$$\begin{cases} Y_0 = X_0 = 4, \\ Y_2 = X_1 = 8, \\ Y_4 = X_2 = 0, \\ Y_6 = X_3 = -8. \end{cases}$$

$$\begin{cases} Z_0 = X_0 = 4, \\ Z_4 = X_1 = 8, \\ Z_8 = X_2 = 0, \\ Z_{12} = X_3 = -8. \end{cases}$$

如果取参数 $M=17$, $N=8$, $\alpha=2$ 的 NTT, 对 $\{y_n\}$ 进行变换，得到

$$\{Y_k\} \equiv (4,\ -8,\ 8,\ -4,\ 0,\ 1,\ -8,\ -2) \quad (\text{mod} 17).$$

如果取参数 $M=17$, $N=16$, $\alpha=\sqrt{2}\equiv 6$ 的 NTT, 对 $\{z_n\}$ 进行变换，得到

$$\{Z_k\} \equiv (4,\ -2,\ -8,\ -1,\ 8,\ -4,\ -4,\ 4,\ 0,\ 8,\ 1,\ 2,\ -8,\ 2,\ -2,\ -1) \pmod{17}.$$

由此知，当补零将序列长度增加时，变换点数增加，但在 $\frac{k}{r}$ 为整数处，数值不变. 如图 4 所示.

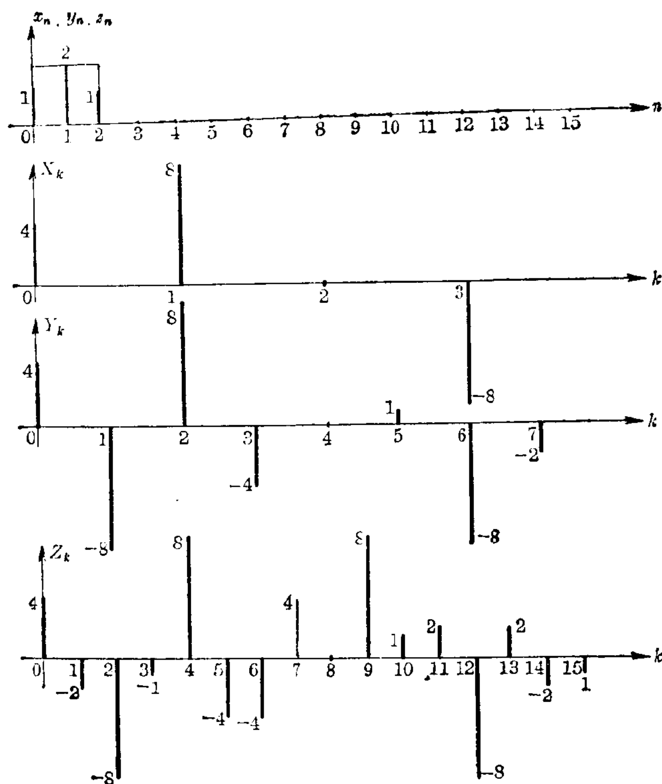


图 4

另一种延伸是将序列 $x_n\ (n=0,\ 1,\ \cdots,\ N-1)$ 周期重复，即作如下一长为 rN (r 为正整数) 的序列:

$$y_n = x_{\langle n\rangle_N} \quad (n=0,\ 1,\ 2,\ \cdots,\ rN-1). \tag{16}$$

假设 α 对模 M 的阶数为 rN，那么 α^r 对模 M 的阶数为 N。于是

$$Y_k \equiv \sum_{n=0}^{rN-1} y_n\alpha^{nk} = \sum_{n=0}^{rN-1} x_{\langle n\rangle_N}\alpha^{nk} = \sum_{n=0}^{N-1} x_n \sum_{l=0}^{r-1} (\alpha^r)^{\frac{k(n+lN)}{r}}$$

$$= \sum_{n=0}^{N-1} x_n(\alpha^r)^{\frac{kn}{r}} \sum_{l=0}^{r-1} (\alpha^r)^{\frac{k}{r}lN} = \sum_{n=0}^{N-1} x_n(\alpha^r)^{\frac{kn}{r}} \sum_{l=0}^{r-1} q^{lN}$$

$$(\bmod M) \quad (k=0,\ 1,\ \cdots,\ rN-1),$$

其中 $q=(\alpha^r)^{\frac{k}{r}}$. 由于

$$\sum_{l=0}^{r-1} q^{lN} \equiv \begin{cases} r, & \dfrac{k}{r}\text{ 为正整数,} \\ 0, & \text{其它,} \end{cases} \quad (\bmod M).$$

故

$$Y_k \equiv \begin{cases} rX_{\frac{k}{r}}, & \dfrac{k}{r}\text{ 为正整数,} \\ 0, & \text{其它,} \end{cases} \quad (\bmod M)$$

$$(k=0,\ 1,\ \cdots,\ rN-1). \tag{17}$$

这就是所求的结果.

例 3 将例 2 的序列作周期重复:

$N=4$, $\{x_n\}=(1,\ 2,\ 1,\ 0)$,

$N=8$, $\{y_n\}=(1,\ 2,\ 1,\ 0,\ 1,\ 2,\ 1,\ 0)$,

$N=16$, $\{z_n\}=(1,\ 2,\ 1,\ 0,\ 1,\ 2,\ 1,\ 0,\ 1,\ 2,\ 1,\ 0,\ 1,\ 2,\ 1,\ 0)$.

取 NTT 的参数为 $M=17$, $N=4$, $\alpha=4$, 将 $\{x_n\}$ 变换，得

$$\{X_k\} \equiv (4,\ 8,\ 0,\ -8) \quad (\bmod 17),$$

由(17)式，得到

$$\{Y_k\} \equiv (8,\ 0,\ 16,\ 0,\ 0,\ 0,\ -16,\ 0)$$
$$\equiv (8,\ 0,\ -1,\ 0,\ 0,\ 0,\ 1,\ 0)\ (\bmod 17),$$

$$\{Z_k\} \equiv (-1,\ 0,\ 0,\ 0,\ -2,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 2,\ 0,\ 0,\ 0) \pmod{17},$$

$\{x_n\}$, $\{X_k\}$, $\{y_n\}$, $\{Y_k\}$表示于图 5 中.

如果取参数 $M=17$, $N=8$, $\alpha=2$ 的 NTT 对 $\{y_n\}$ 进行变换, 以及取参数 $M=17, N=16, \alpha=\sqrt{2}=6$ 的 NTT 对$\{z_n\}$进行变换, 将得到与上面相同的结果. 读者可自行推导.

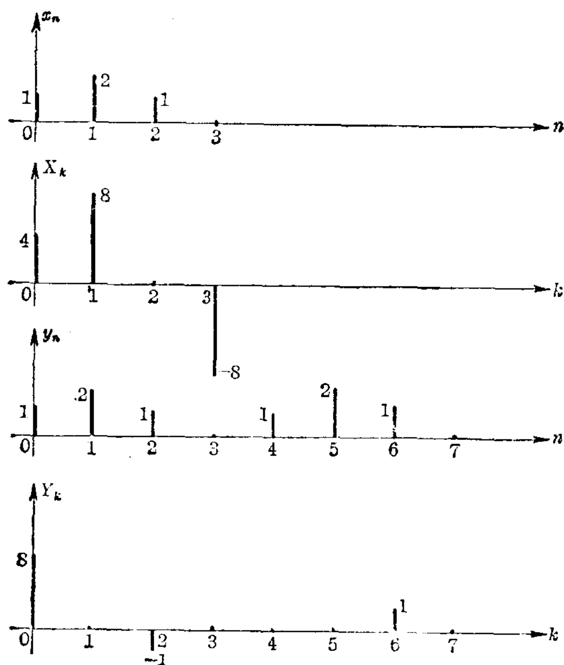


图 5

—6—

在整数环 Z_M 上 N 阶本原单位根的计算方法

我们在 **4** 中详细的讨论了 Z_M 上存在具有循环卷积特性的一对可逆变换的条件，α 是一个整数，显然它要比 DFT 中的 W_N 简单得多，这样 NTT 就克服了 DFT 由于基本函数复杂而带来的一系列缺点. 在 **5** 中，我们详细讨论了 NTT 的性质，读者已经看到，NTT 的性质和 DFT 的性质类似. NTT 和 DFT 一样是一种线性正交变换，并且具有 DFT 一样的快速算法，做一次快速数论变换($N=r_1\cdot r_2\cdot\cdots\cdot r_n$)，大约需要 $N\cdot(r_1+r_2+\cdots+r_n)$ 次算术运算. 如果 $\alpha=2$ 或 2 的幂，那么在二进制计算机上作变换时就可以不用乘法，仅为移位操作.

现在我们讨论，给定 $M=p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s}$ 和 N ($N|O(M)$) 后(从下一节可以知道，M 和 N 的选择将根据我们所计算问题的性质)，具体地来计算适合 NTT 的 α. 根据 **4** 的定理 1，α 必需同时是模 M 及模 p_i ($i=1, 2, \cdots, s$) 的 N 阶本原单位根. 计算 α 的步骤基本上同 **4** 中定理 4 的证明方法. 结果我们可以知道，共有 $\varphi^s(N)$ 个 α 适合我们的需要，从 $\varphi^s(N)$ 个 α 中任意选择一个，就可以和给定的 M, N 一起组成 NTT. 这里给出计算 α 的两种方法.

设 $M=p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s}$，$N$ 是 $O(M)$ 的一个约数.

一、算 法 一

这种方法分为三步：第一步对模 p_i 求出 N 阶本原单位根

$\beta_i\,(i=1,\ 2,\ \cdots,\ s)$；第二步对模 $p_i^{l_i}$ 求出 N 阶本原单位根 $\alpha_i\,(i=1,\ 2,\ \cdots,\ s)$；第三步对模 M 求出 N 阶本原单位根 α. 由 **4** 中定理 4 求出的 α 即满足要求.

第一步：由于 p_i 为奇素数(如果 M 为偶数，那么 2 是它的一个因子，由 **4** 中定理 4，只能给出长度 $N=1$ 的变换，这没有什么意思，所以 M 必须为奇数，从而知 p_i 为奇素数，可参阅 **7**)，故在 Z_{p_i} 上存在主根，记为 g_i. 取 $\beta_i=g_i^{\frac{p_i-1}{N}}$，此 β_i 即为对模 p_i 的 N 阶本原单位根.

第二步：由于 $p_i \mid \beta_i^N-1$，故设 $p_i^{t_i} \mid \beta_i^N-1$，而 $p_i^{t_i+1} \nmid \beta_i^N-1$ $(t_i\geqslant 1)$ ($p_i^{t_i} \mid \beta_i^N-1$ 但 $p_i^{t_i+1} \nmid \beta_i^N-1$，简记为 $p_i^{t_i} \| \beta_i^N-1$)，如果 $t_i\geqslant l_i$，那么此 β_i 即为对模 $p_i^{l_i}$ 的 N 阶单位根. 若 $t_i<l_i$ (这里设 $l_i>1$)，记

$$\beta_i^{(2)}=\beta_i+d_ip_i^{t_i}$$

可如下法那样，逐步求出 d_i，使 $\beta_i^{(2)}$ 为对模 $p_i^{l_i}$ 的 N 阶单位根.

首先选取 d_i，使 $p_i^{t_i+1} \mid [\beta_i^{(2)}]^N-1$，即使

$$p_i^{t_i+1} \mid (\beta_i+d_ip_i^{t_i})^N-1,$$

亦即使 $$(\beta_i+d_ip_i^{t_i})^N-1\equiv 0 \pmod{p_i^{t_i+1}}.$$

将上式左端用二项式定理展开，得

$$\beta_i^N-1+N\beta_i^{N-1}d_ip_i^{t_i}+\binom{N}{2}\beta_i^{N-1}d_i^2p_i^{2t_i}+\cdots\equiv 0 \pmod{p_i^{t_i+1}}.$$

记 $\beta_i^N-1=l_ip_i^{t_i}$，其中，l_i 为一整数，并且 $p_i \nmid l_i$. 于是上式便有

$$l_ip_i^{t_i}+N\beta_i^{N-1}d_ip_i^{t_i}=p_i^{t_i}(l_i+N\beta_i^{N-1}d_i)\equiv 0 \pmod{p_i^{t_i+1}},$$

故 $$l_i+N\beta_i^{N-1}d_i\equiv 0 \pmod{p_i}.$$

由于 β_i 是模 p_i 的 N 阶单位根，而 $N \mid O(M)$，所以 $p_i \nmid N\beta_i^{N-1}$，

又由于 p_i 是素数，故 $N\beta_i^{N-1}$ 与 p_i 互素，从而 $N\beta_i^{N-1}$ 在环 Z_{p_i} 中存在逆元，记为 $(N\beta_i^{N-1})^{-1}$. 这样，解上同余方程，得

$$d_i \equiv -(N\beta_i^{N-1})^{-1} l_i \pmod{p_i}.$$

这样求出的 d_i，代入 $\beta_i^{(2)}$ 的式子后，便有

$$[\beta_i^{(2)}]^N \equiv 1 \pmod{p_i^{t_i+1}}.$$

如果 $t_i+1=l_i$，那么 $\beta_i^{(2)}$ 是模 $p_i^{l_i}$ 的 N 阶单位根，$\beta_i^{(2)}$ 就是所要求的. 如果 $t_i+1<l_i$，再令

$$\beta_i^{(3)} = \beta_i^{(2)} + d_i' p_i^{t_i+1},$$

重复上述步骤，确定 d_i'，便得

$$[\beta_i^{(3)}]^N \equiv 1 \pmod{p_i^{t_i+2}}.$$

继续有限步后，便可求出 $\alpha_i=\beta_i^{(m)}$，使 α_i 对模 $p_i^{l_i}$ 的阶数为 N.

对每一个 $i(i=1, 2, \cdots, s)$，都求出 α_i.

第三步：由第二步已求得模 $p_i^{l_i}(i=1, 2, \cdots, s)$ 的 N 阶单位根 α_i，用孙子定理求联立同余方程组

$$\alpha \equiv \alpha_i \pmod{p_i^{l_i}} \quad (i=1, 2, \cdots, s)$$

的解，其解为 $$\alpha \equiv \sum_{i=1}^{s} M_i' M_i \alpha_i \pmod{M}.$$

其中 $M_i' M_i \equiv 1 \pmod{p_i^{l_i}}$ $(i=1, 2, \cdots, s)$. 此 α 即为所求.

例 1 设 $M=5^2\cdot 13^2$, $N=4$, 求 α.

【解】 第一步先求 β_1, β_2. β_1 是模 5 的 4 阶单位根，β_2 是模 13 的 4 阶单位根，求得为

$$\beta_1=2, 3; \quad \beta_2=5, 8$$

(这一步可查表求主根，然后求 β_i).

第二步：当 $\beta_1=2$ 时，$2^4-1=15=3\cdot 5$，不含有 5^2，故令 $\beta_1^{(2)}=2+d_1\cdot 5$，确定 d_1，使 $\beta_1^{(2)}$ 为 Z_{5^2} 中的 4 阶单位根.

$$[\beta_1^{(2)}]^4-1=(2+5d_1)^4-1=15+4\cdot 8\cdot 5d_1 \equiv 0 \pmod{5^2},$$

即 $$3+32d_1\equiv 0 \pmod{5}.$$
解此同余方程，得 $d_1=1$，故

$$\beta_1^{(2)}=7.$$

可以验证，7 对模 25 的阶数为 4，故取 $\alpha_1=7$。

当 $\beta_1=3$ 时，$3^4-1=80=5\cdot 16$ 不含 5^2，故令

$$\beta_1^{(2)}=3+5d_1',$$

确定 d_1'，使 $[\beta_1^{(2)}]^4-1\equiv 0 \pmod{5^2}$，得到 $d_1'=3$，故 $\beta_1^{(2)}=18$。不难验证，18 对模 25 的阶数为 4，故又可取 $\alpha_1=18$。

在 Z_{5^2} 中，有两个 4 阶单位根 7，18。

同样可求出在 Z_{13^2} 中有两个 4 阶单位根 70，99。

第三步：在 Z_M 中求出相应的 4 阶单位根．这可从如下四组联立同余方程中去找．

$$\begin{cases}\alpha\equiv 7 & \pmod{5^2},\\ \alpha\equiv 70 & \pmod{13^2};\end{cases}\qquad \begin{cases}\alpha\equiv 7 & \pmod{5^2},\\ \alpha\equiv 99 & \pmod{13^2};\end{cases}$$

$$\begin{cases}\alpha\equiv 18 & \pmod{5^2},\\ \alpha\equiv 70 & \pmod{13^2};\end{cases}\qquad \begin{cases}\alpha\equiv 18 & \pmod{5^2},\\ \alpha\equiv 99 & \pmod{13^2}.\end{cases}$$

应用孙子定理，求出的四个 α 为

$$268,\ 1282,\ 2943,\ 3957.$$

用这四个 α 的任一个，均可与 $M=5^2\cdot 13^2$，$N=4$ 一起构成 NTT。

二、算 法 二

这种算法与算法一一样，分为三步，第一、三步相同，只是第二步不同。

第一步：求出 Z_{p_i} 中的 N 阶单位根 β_i $(i=1, 2, \cdots, s)$。

第二步：令

$$\alpha_i = \beta_i^{p_i^{l_i-1}},$$

可以证明，α_i 是对模 $p_i^{l_i}$ 的 N 阶单位根.

证明 由于 $\beta_i^N \equiv 1 \pmod{p_i}$，故可写作

$$\beta_i^N = 1 + q_i p_i \quad (q_i \text{ 为整数}).$$

于是，
$$\alpha_i^N = [\beta_i^{p_i^{l_i-1}}]^N = [\beta_i^N]^{p_i^{l_i-1}} = (1+q_i p_i)^{p_i^{l_i-1}}$$
$$= 1 + \sum_{k=1}^{p_i^{l_i-1}} \binom{p_i^{l_i-1}}{k} (q_i p_i)^k.$$

设 $p_i^{b_k}$ 是上式第 k 项所含 p_i 的最高幂，即设

$$p_i^{b_k} \Big\| \binom{p_i^{l_i-1}}{k} (q_i p_i)^k \quad (k = 1,\ 2,\ \cdots,\ p_i^{l_i-1}).$$

由于

$$\binom{p_i^{l_i-1}}{k} (q_i p_i)^k = \frac{p_i^{l_i-1}(p_i^{l_i-1}-1)\cdots(p_i^{l_i-1}-k+1)}{1\cdot 2\cdots k} q_i^k p_i^k,$$

所以，显然 $$b_k \geqslant l_i - 1 + k - \sum_{\lambda=1}^{\infty} \left[\frac{k}{p_i^\lambda}\right].$$

其中 $\sum\limits_{\lambda=1}^{\infty} \left[\frac{k}{p_i^\lambda}\right]$ 是 $k! = 1\cdot 2\cdot\cdots\cdot k$ 中所含 p_i 的次数. 由于

$$\left[\frac{k}{p_i^\lambda}\right] \leqslant \frac{k}{p_i^\lambda},$$

故 $$b_k \geqslant l_i - 1 + k - \sum_{\lambda=1}^{\infty} \frac{k}{p_i^\lambda} = l_i - 1 + k - k\cdot\frac{\frac{1}{p_i}}{1-\frac{1}{p_i}}$$
$$= l_i - 1 + k - \frac{k}{p_i - 1} = l_i - 1 + k\cdot\frac{p_i - 2}{p_i - 1} > l_i - 1.$$

这表示 $p_i^{l_i} | \alpha_i^N - 1$. 从而有

$$\alpha_i^N \equiv 1 \pmod{p_i^{l_i}}.$$

下面再证明 α_i 对模 $p_i^{l_i}$ 的阶数是 N. 令 d 为 α_i 对模 $p_i^{l_i}$ 的阶数，则

$$d|N.$$

显然，这时也有

$$\alpha_i^d \equiv 1 \pmod{p_i}.$$

但由 Fermat 定理，有

$$\beta_i^{p_i-1} \equiv 1 \pmod{p_i},$$

即

$$\beta_i^{p_i} \equiv \beta_i \pmod{p_i}.$$

从而有

$$\beta_i^{p_i^2} \equiv \beta_i^{p_i} \equiv \beta_i \pmod{p_i},$$

$$\cdots\cdots$$

$$\beta_i^{l_i-1} \equiv \beta_i \pmod{p_i},$$

即 $\alpha_i \equiv \beta_i \pmod{p_i}$，这样就有

$$\beta_i^d \equiv 1 \pmod{p_i}.$$

由于 β_i 对模 p_i 的阶数为 N，故 $N|d$. 这就表示 $d=N$.

第三步：用孙子定理求 α，同算法一.

例 2 设 $M=5^2 \cdot 13^2$，$N=4$，求 α.

【解】 第一步同例 1，得到：

在 Z_5 中 4 阶单位根为 2，3；在 Z_{13} 中 4 阶单位根为 5，8.

第二步：由 $\alpha_i=\beta_i^{l_i-1}$ 得到：

$\alpha_1=2^5 \equiv 7 \pmod{25}$，　$\alpha_2=5^{13} \equiv 70 \pmod{13^2}$，

$\alpha_1=3^5 \equiv 18 \pmod{25}$，　$\alpha_2=8^{13} \equiv 99 \pmod{13^2}$.

第三步，用孙子定理，便得到与例 1 相同的结果.

由以上两算法，可得如下定理：

定理 1 设 $M=p_1^{l_1} \cdot p_2^{l_2} \cdots p_s^{l_s}$，$N|O(M)$，则共有 $\varphi^s(N)$ 个 α 适合 NTT 的需要.

从算法一和算法二中可以看出，不同的 β_i 得到不同的 α_i，对每个 p_i 来说，共有 $\varphi(N)$ 个 β_i，从而有 $\varphi(N)$ 个 α_i，配成联立同余方程组，共有 $\varphi^s(N)$ 组，每组有且只有一个解 α，从而有 $\varphi^s(N)$ 个 α. 这 $\varphi^s(N)$ 个 α 中的任意一个均可与 M，N 一起作成 NTT.

—7—

M、N、A 的选择

4 中详细的讨论了数论变换的原理及构成数论变换的参数 M, N, α 所应满足的条件. 6 中讨论了 Z_M 中的所有可能的数论变换. 从本节开始, 将从实用的观点出发, 讨论几种特殊的数论变换. 首先从 M, N, α 的选择开始.

一、对 M、N、A 的一般要求

为了使 NTT 具有快速演算的效果, 通常对 M、N、α 的要求是:

1° 变换长度 N 必须适合 FFT 类型的快速演算, 因而要求 N 是高度复合的数. 当 $N=2^m$ 时, 就能满足这样的要求. 同时, 由于 N 表示输入信号采样点的个数, 所以不能过小.

2° 数论变换的一个特点是用一个整数 α 代替 DFT 中的 $W_N=e^{-j\frac{2\pi}{N}}$, FFT 需要大量的复乘, 而 NTT 只须作 α 的方幂的乘法. 如果能选择 α, 使得乘 α 的幂是一种简单运算, 那么就能起到节省运算的目的. 当 α 的方幂的二进制表示位数很小时, 就能起到这样的效果. 如果 α 能取作 2 或 2 的幂, 是最好的情况, 这时在二进制计算机上作 2 的方幂的乘法时, 仅为移位操作.

3° 为了便于模 M 的运算, 当用二进制表示 M 时, 其位数(一般称为字长)越小越好. 但 M 的值不能过小, 以防溢出.

二、对M的选择

变换长度 N 与模 M 的关系是 $N|O(M)$. 因此

1° 当 M 是偶数时, 2 是 M 的一个因子, 因此, N 只能取作 1, 这没有什么意义. 因此, M 不能是偶数.

2° M 取作大于 2 的素数. 这时 M 是一奇数. 由于 $(2, M)=1$, 故根据 Fermat 定理, 有

$$2^{M-1}\equiv 1 \pmod{M}.$$

因此, N 可取 $M-1$ 的任何因子, 这时 $\alpha=2$ 或 2 的幂, $N_{max}=M-1$. 例如, $M=17$, $N|16$, 可取 4, 8, 16, 相应的 α 值为 4, 2, $\sqrt{2}$. 虽然 M 取作奇素数时可以适合 NTT 的要求, 主要问题是 N 未必是高度复合数, 更未必有 2^m 的形式.

3° M 取作 Mersenne 数.

设 $$M=2^k-1, \quad k \text{ 为自然数}.$$

显然 M 是一个奇整数. 令 $k=pq$ (p 为素数), 那么

$$2^k-1=2^{pq}-1=(2^p)^q-1\equiv 0 \pmod{2^p-1},$$

所以 2^p-1 是 2^k-1 的一个因子, 从而最大可能变换长度决定于 2^p-1. 如果取

$$M=2^p-1, \quad p \text{ 为素数},$$

这样的数称为 Mersenne 数. 取 Mersenne 数作为模 M, 是适合 NTT 的要求的. 以 Mersenne 数为模的数论变换, 叫做 Mersenne 数变换, 简记为 MNT. 对于 MNT, $\alpha=2$, $N=p$ 或者 $\alpha=-2$, $N=2p$, 这将在下节介绍.

4° M 取作 Fermat 数.

设 $$M=2^k+1, \quad k \text{ 为自然数}.$$

M 也是一个奇整数. 当 k 为奇数时, 设 $k=2t+1$, 由于

$$2^k+1=2^{2t+1}+1=(2+1)(2^{2t}-2^{2t-1}+\cdots-2+1)$$
$$=3(2^{2t}-2^{2t-1}+\cdots-2+1),$$

故
$$3\mid 2^k+1.$$

这时 $N_{max}=2$, 显然不合实际需要.

当 $k=s\cdot 2^t$(s 为奇整数, $t=1, 2, 3\cdots$)时,
$$M=2^{s\cdot 2^t}+1,$$

由于 $$2^{s\cdot 2^t}+1=(2^{2^t})^s+1\equiv(-1)^s+1=0 \quad (\bmod 2^{2^t}+1),$$

即
$$2^{2^t}+1\mid 2^{s\cdot 2^t}+1,$$

所以变换长度决定于 $2^{2^t}+1$. 取 $F_t=2^{2^t}+1$ 为模 M,
$$M=F_t=2^b+1, \quad b=2^t \quad (t=0, 1, 2, \cdots),$$

这样的数叫做 Fermat 数. 以 Fermat 数 F_t 作为模 M 的数论变换叫做 Fermat 数变换, 记作 FNT. 对于 FNT, $N=2b=2^{t+1}$, $\alpha=2$; $N=4b=2^{t+2}$, $\alpha=\sqrt{2}$, 均能满足要求. 关于 FNT, 将在 **9** 中介绍.

综上所述, 模 M 取作 Fermat 数, 是目前找到的较合适的模数.

三、M 选取的另一个考虑

如果我们用 NTT 的循环卷积特性来计算数字循环卷积
$$y_n=\sum_{k=0}^{N-1}x_k h_{\langle n-k\rangle_N} \quad (n=0, 1, \cdots, N-1), \qquad (1)$$

由于 NTT 所用的运算是模运算, 因此, 这样求得的卷积值 y_n 乃是模 M 的同余值, 亦即
$$\sum_{k=0}^{N-1}x_k h_{\langle n-k\rangle_N}\equiv y_n \quad (\bmod M).$$

y_n 所属的剩余类中的每一个数 y_n+rM (r 为整数) 均满足上式. 倒底那一个值才是 (1) 的真值呢? 这个问题可用选择模

M 得到解决.

在数字滤波的多数情况下,(1)中的 $\{h_n\}$ 表示单位脉冲响应, $\{x_n\}$ 表示输入信号, $|h_n|_{\max}$ 和 $|x_n|_{\max}$ 通常是已知的. 因此,能够选择模 M 使得下式成立,

$$|y_n| \leqslant \min\left\{|x_n|_{\max}\sum_{k=0}^{N-1}|h_k|,\ |h_n|_{\max}\sum_{k=0}^{N-1}|x_k|\right\} < \frac{M}{2} \quad (n=0, 1, \cdots, N-1). \tag{2}$$

由于当 $-\frac{M}{2} < a < \frac{M}{2}$ 时, $a = r_a$(a 为整数), 其中 $|r_a| < \frac{M}{2}$, r_a 为 a 模 M 的绝对最小剩余. 因此,在用 NTT 计算(1)时,由于有(2)存在,也就是说有

$$\left|\sum_{k=0}^{N-1} x_k h_{\langle n-k\rangle_N}\right| < \frac{M}{2} \quad (n=0, 1, \cdots, N-1)$$

成立,因此,只需在计算结果中取绝对最小剩余,就得到(1)的真值. 具体例子可参阅 **8** 或 **9**.

所以模 M 必需这样选择,即满足

$$\min\left\{|x_n|_{\max}\sum_{k=0}^{N-1}|h_k|,\ |h_n|_{\max}\sum_{k=0}^{N-1}|x_k|\right\} < \frac{M}{2} \quad (n=0, 1, \cdots, N-1). \tag{2'}$$

—8—

Mersenne 数变换(MNT)

以 Mersenne 数 M_p 为模 M 的数论变换为 Mersenne 数变换.

$$M=M_p=2^p-1,\quad p\text{ 为素数.}$$

M_p 可能是素数，如

$$M_2=2^2-1=3,$$

$$M_3=2^3-1=7,$$

$$M_5=2^5-1=31,$$

$$M_7=2^7-1=127.$$

但也可能是复合数，如 $M_{11}=2^{11}-1=2047=23\times 89$.

一、两 个 引 理

引理 1 当 M_p 为素数时，p 必为素数.

证明 如果不然，设 $p=ab$（$a>1$，$b>1$ 为整数），那么 $2^p=2^{ab}-1=(2^a)^b-1\equiv 0(\bmod 2^a-1)$，这表示 $2^a-1|2^{ab}-1$. 故 2^p-1 为非素数. 引理得证.

引理 2 当 p 为奇素数时，2^p-1 的每一个素因子均具有 $2pk+1$ 的形式. 其中 k 为正整数.

证明 设 2^p-1 的任一素因子为 q，于是

$$2^p\equiv 1 \quad (\bmod q).$$

设 d 为 2 对模 q 的阶数，于是 $d|p$. 由于 p 是素数，故 $p=d$. 又由于 2^p-1 是奇数，q 也是奇数，从而 $(2,q)=1$. 于是由

Fermat 定理，有 $2^{q-1}\equiv 1(\bmod q)$，因此 $p|q-1$. 但因 $q-1$ 是偶数，故 $q-1=2kp$，亦即

$$q=2kp+1.$$

k 为正整数．证毕．

二、Mersenne 数变换

取 Mersenne 数为模，$M=M_p=2^p-1$，p 为素数，可以证明 N, α 可取如下值：

α	N	N^{-1}
2	p	$M_p-\frac{M_p-1}{p}$
-2	$2p$	$M_p-\frac{M_p-1}{2p}$

1. $N=p$, $\alpha=2$ 的情况*.

首先证明 $p|M_p-1$，即证明 $M_p-\frac{M_p-1}{p}$ 是一整数．由于 $(2, p)=1$，故由 Fermat 定理，$2^{p-1}\equiv 1(\bmod p)$．故 $2^p-2\equiv 0(\bmod p)$，即 $p|M_p-1$．又

$$NN^{-1}=p\left(M_p-\frac{M_p-1}{p}\right)\equiv 1 \quad (\bmod M_p).$$

由于 $2^p\equiv 1(\bmod M_p)$，p 为素数，故 2 对模 M_p 的阶是 p. 再设 q 是 M_p 的任一素因子，由引理 2 的证明可知，2 对模 q 的阶数也是 p，故根据 **4** 中定理 1，知如下变换成立：

---

* 用 **4** 中定理 3 来证明$\{\alpha=2, N=p\}$ 及 $\{\alpha=-2, N=2p\}$ 适合 NTT 的条件，请参阅 **12**.

设 $x_n \in Z_M$ $(n=0, 1, \cdots, p-1)$，$M=M_p=2^p-1$，p 为素数，则

$$X_k \equiv \sum_{n=0}^{p-1} x_n 2^{nk} (\bmod M_p) \quad (k=0, 1, \cdots, p-1), \qquad (1)$$

$$x_n \equiv p^{-1} \sum_{k=0}^{p-1} X_k 2^{-nk} (\bmod M_p) \quad (n=0, 1, \cdots, p-1). \qquad (2)$$

2. $N=2p$，$\alpha=-2$.

取 $M=M_p=2^p-1$，p 为素数，由引理 2，M_p 的任一素因子为 $q=2kp+1$，故 N 可取 $q-1$ 的任一因子，特别可取 $N=2p$.

由于

$$(-2)^N=(-2)^{2p}=2^{2p}=(2^p)^2 \equiv 1 \quad (\bmod M_p),$$

$$(-2)^{\frac{N}{2}}=(-2)^p=-(2^p) \equiv -1 \quad (\bmod M_p),$$

所以 $\alpha=-2$ 对模 M_p 的阶数是 $N=2p$. 又设 q 是 M_p 的任一素因子，并设 $\alpha=-2$ 对模 q 的阶为 d，由于

$$(-2)^{2p} \equiv 1 \quad (\bmod q),$$

故 $d|2p$. 但由于 p 是素数，所以只能有 $d=2p$，$d=2$，$d=p$，但后两种情况不能发生，否则将与 $(-2)^p \equiv -1 (\bmod q)$ 矛盾. 所以 $d=2p$. 这就证明了 $\alpha=-2$ 对 M_p 的任一素因子 q 的阶是 $2p$. 故由 4 中定理 1，知 $\{N=2p, \alpha=-2\}$ 满足 NTT 的条件. 另外，显然可证 $N^{-1}=M_p-\dfrac{M_p-1}{2p}$ 是 N 在 Z_{M_p} 中的逆元 $\left(\dfrac{M_p-1}{2p}\right.$ 是整数，这由 $2^p \equiv 2 (\bmod 2p)$ 可知$\left.\right)$. 因此如下变换成立：

设 $x_n \in Z_{M_p}$，$M=M_p=2^p-1$，p 是素数，则

$$X_k \equiv \sum_{n=0}^{N-1} x_n (-2)^{nk} (\bmod M_p)$$

$$(k=0, 1, \cdots, N-1), \qquad (3)$$

$$x_n \equiv N^{-1}\sum_{k=0}^{N-1} X_k(-2)^{-nk} (\mathrm{mod} M_p)$$

$$(n=0,\ 1,\ \cdots,\ N-1). \tag{4}$$

其中，$\qquad N=2p,\quad N^{-1}=M_p-\dfrac{M_p-1}{2p}.$

例 试用 Mersenne 数变换计算如下两个序列

$$\{x_5\}=\begin{bmatrix}1\\2\\0\\-2\\1\end{bmatrix},\qquad \{h_5\}=\begin{bmatrix}1\\-2\\1\\0\\1\end{bmatrix}$$

的循环卷积

$$y_n=\sum_{k=0}^{4} x_k h_{\langle n-k\rangle_5}\quad (n=0,\ 1,\ 2,\ 3,\ 4).$$

【解】 先取 M. 由 **7** 中(2)式

$$|x_n|_{\max}\sum_{k=0}^{4}|h_k|=2\cdot 5=10\quad (n=0,\ 1,\ 2,\ 3,\ 4).$$

取 M, 使 $10<\dfrac{M}{2}$, 故可取:

$$M=M_5=2^5-1=31,\quad \alpha=2,\quad N=p=5,$$

这时 $\qquad N^{-1}=p^{-1}=M_p-\dfrac{M_p-1}{5}=25.$

于是

$$T_5=\begin{bmatrix}1&1&1&1&1\\1&\alpha&\alpha^2&\alpha^3&\alpha^4\\1&\alpha^2&\alpha^4&\alpha^6&\alpha^8\\1&\alpha^3&\alpha^6&\alpha^9&\alpha^{12}\\1&\alpha^4&\alpha^8&\alpha^{12}&\alpha^{16}\end{bmatrix}=\begin{bmatrix}1&1&1&1&1\\1&2&2^2&2^3&2^4\\1&2^2&2^4&2^6&2^8\\1&2^3&2^6&2^9&2^{12}\\1&2^4&2^8&2^{12}&2^{16}\end{bmatrix}$$

$$\equiv\begin{bmatrix}1&1&1&1&1\\1&2&4&8&16\\1&4&16&2&8\\1&8&2&16&4\\1&16&8&4&2\end{bmatrix}\pmod{31}.$$

因为 $\alpha^{-1}=2^{-1}\equiv16\pmod{31}$, $N^{-1}=25$, 故

$$T_5^{-1}\equiv N^{-1}\begin{bmatrix}1&1&1&1&1\\1&\alpha^{-1}&\alpha^{-2}&\alpha^{-3}&\alpha^{-4}\\1&\alpha^{-2}&\alpha^{-4}&\alpha^{-6}&\alpha^{-8}\\1&\alpha^{-3}&\alpha^{-6}&\alpha^{-9}&\alpha^{-12}\\1&\alpha^{-4}&\alpha^{-8}&\alpha^{-12}&\alpha^{-16}\end{bmatrix}$$

$$\equiv25\begin{bmatrix}1&1&1&1&1\\1&2^{-1}&2^{-2}&2^{-3}&2^{-4}\\1&2^{-2}&2^{-4}&2^{-6}&2^{-8}\\1&2^{-3}&2^{-6}&2^{-9}&2^{-12}\\1&2^{-4}&2^{-8}&2^{-12}&2^{-16}\end{bmatrix}$$

$$\equiv25\begin{bmatrix}1&1&1&1&1\\1&2^{4}&2^{8}&2^{12}&2^{16}\\1&2^{8}&2^{16}&2^{24}&2^{32}\\1&2^{12}&2^{24}&2^{36}&2^{48}\\1&2^{16}&2^{32}&2^{48}&2^{64}\end{bmatrix}$$

$$\equiv25\begin{bmatrix}1&1&1&1&1\\1&16&8&4&2\\1&8&2&16&4\\1&4&16&2&8\\1&2&4&8&16\end{bmatrix}\pmod{31}.$$

因此

$$\begin{bmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{bmatrix} \equiv T_5 \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 \\ 1 & 4 & 16 & 2 & 8 \\ 1 & 8 & 2 & 16 & 4 \\ 1 & 16 & 8 & 4 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 0 \\ -2 \\ 1 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 2 \\ 5 \\ 13 \\ -11 \\ -4 \end{bmatrix} \quad (\bmod 31).$$

同理，可算得

$$\begin{bmatrix} H_0 \\ H_1 \\ H_2 \\ H_3 \\ H_4 \end{bmatrix} \equiv T_5 \begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \\ h_4 \end{bmatrix} \equiv \begin{bmatrix} 1 \\ -14 \\ -14 \\ -9 \\ 10 \end{bmatrix} \quad (\bmod 31).$$

利用循环卷积特性 $Y_k = X_k \cdot H_k (k=0, 1, 2, 3, 4)$，有

$$\begin{bmatrix} Y_0 \\ Y_1 \\ Y_2 \\ Y_3 \\ Y_4 \end{bmatrix} \equiv \begin{bmatrix} 2 \\ -70 \\ -182 \\ 99 \\ -40 \end{bmatrix} \equiv \begin{bmatrix} 2 \\ -8 \\ 4 \\ 6 \\ -9 \end{bmatrix} \quad (\bmod 31).$$

再利用逆变换，得

$$
\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = T_5^{-1} \begin{bmatrix} Y_0 \\ Y_1 \\ Y_2 \\ Y_3 \\ Y_4 \end{bmatrix} = 25 \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 16 & 8 & 4 & 2 \\ 1 & 8 & 2 & 16 & 4 \\ 1 & 4 & 16 & 2 & 8 \\ 1 & 2 & 4 & 8 & 16 \end{bmatrix} \begin{bmatrix} 2 \\ -8 \\ 4 \\ 6 \\ -9 \end{bmatrix}
$$

$$
= 25 \begin{bmatrix} -5 \\ -88 \\ 6 \\ -26 \\ -94 \end{bmatrix} \equiv \begin{bmatrix} 30 \\ -30 \\ -36 \\ -30 \\ 6 \end{bmatrix} \quad (\mathrm{mod}\,31).
$$

取其绝对最小剩余，得到

$$
\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} -1 \\ 1 \\ -5 \\ 1 \\ 6 \end{bmatrix}.
$$

这就是所求卷积的真值. 不难用循环卷积的定义(**1** 中(2)式)验证.

对于 Mersenne 数变换, $\alpha=2$ 或 -2, 这满足对根 α 的要求，对 α 的方幂的乘法仅是移位操作. 其变换长度为 $N=p$ 或 $2p$. 这一般适合于短卷积的计算. 对于长序列的卷积, 可用 **14** 中的方法(一维卷积多维处理). 但是 $N=p$ 是素数, $N=2p$ 虽是复合数, 但非高度复合数, 特别不是 2^m 形式的数, 因此, MNT 没有 FFT 类型的快速算法, 这是 MNT 的主要缺点.

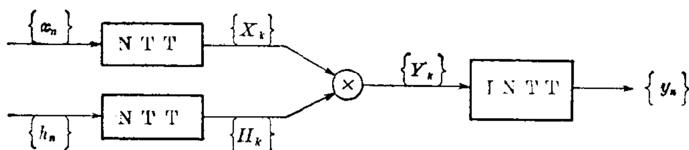
从上面用 MNT 计算循环卷积的例子可知，要用 NTT 计算整数序列 x_n 和 h_n 的循环卷积，其步骤如下:

1° 根据下式选取模 M:

$$\min\left\{|x_n|_{\max}\sum_{k=0}^{N-1}|h_k|,\quad |h_n|_{\max}\sum_{k=0}^{N-1}|x_k|\right\}<\frac{M}{2}$$
$$(n=0,\ 1,\ \cdots,\ N-1);$$

2° 将整数序列 x_n 和 h_n 以 M 为模表示成 Z_M 中的元素；至于 N, 它可能与其它因素有关(如在数字信号处理中，由采样定理决定 N 的最小值)，但必需 $N|O(M)$. 然后由 M, N 决定 α 以构成 NTT;

3° 在 Z_M 中，求 x_n 和 h_n 的循环卷积按下图进行：



4° 最后，将上面得到的序列 y_n 按模 M 取绝对最小剩余，就得到 x_n 和 h_n 的循环卷积的真值.

读者可能发现，1° 与 2° 有矛盾. 由 1°, M 与 N 有关，而由 2°, N 又决定于 M. 对此，只能和其它工程问题一样，要经过数次反复衡量，才能确定 M, N. 不过，好在 M, N 有相当大的选择范围(如 1° 中只确定 M 的最小值，采样定理也只确定 N 的最小值)，我们总能够确定出合适的 M, N.

至于一般的卷积和恒定对角卷积，只需用 **1** 中所指出的方法(引理 1 和引理 2)变成循环卷积，再用上法计算.

—9—

Fermat 数变换(FNT)

称 $F_t=2^b+1$, $b=2^t$ $(t=1, 2, 3, \cdots)$ 为 Fermat 数.

$F_1=2^2+1=5$,

$F_2=2^4+1=17$,

$F_3=2^8+1=257$,

$F_4=2^{16}+1=65537$,

$F_5=2^{32}+1=4,294,967,297=641\cdot6700417$.

由此知, 当 $1\leqslant t\leqslant4$ 时, F_t 是素数, 当 $t\geqslant5$ 时, F_t 可能是复合数.

一、三个引理

引理 1 如果 2^b+1 是素数, 必有 $b=2^t$.

证明 这是因为 $b=s\cdot2^t$ (s 是奇数, 且 $s\neq1$)时,

$$2^{2^t}+1\mid2^{s\cdot2^t}+1.$$

这与假设矛盾,故当 2^b+1 是素数时, $b=2^t$.

这引理的逆是不成立的,如 F_5 就是复合数.

引理 2 如果 $2^b+1(b=2^t)$是非素数,那么它的任何素因子均具有 $q=2bk+1=2^{t+1}k+1$ 的形状,其中 k 为正整数.

证明 设 q 为 2^b+1 的任一素因子 (显然 q 为奇素数), 由于 $2^{2^t}\equiv-1\pmod{q}$, 故

$$2^{2^{t+1}}\equiv1\pmod{q}.$$

设 d 是 2 对模 q 的阶数, 于是有 $d\mid2^{t+1}$. 但因为 2^{t+1} 是 2 的

幂，其最大约数为 2^t，由于

$$2^{2^t}\equiv -1\not\equiv 1 \pmod{q},$$

故可知，以 2^{t+1} 的其它约数 x 为指数时，$2^x\not\equiv 1 \pmod{q}$，所以

$$d=2^{t+1}.$$

另一方面，由于 $(2, q)=1$，故由 Fermat 定理，有

$$2^{q-1}\equiv 1 \pmod{q}.$$

因此 $2^{t+1}|q-1$，从而得到

$$q=2^{t+1}k+1.$$

k 为正整数．证毕．

引理 3 当 $t\geqslant 2$ 时，引理 1 中的 q 可表为

$$q=2^{t+2}h+1$$

的形状，其中 h 为正整数．

证明 由引理 1，知

$$q=2^{t+1}\cdot k+1.$$

当 $t\geqslant 2$ 时，还可进而证明 k 为偶数，即 $k=2h$．由于有

$$q=2^{t+1}\cdot k+1,$$

故当 $t\geqslant 2$ 时，$q\equiv 1 \pmod{8}$．根据二次剩余的理论，当 $q\equiv 1 \pmod{8}$ 时，有

$$2^{\frac{q-1}{2}}\equiv 1 \pmod{q}.$$

而由引理 1，知 $\frac{q-1}{2}=k\cdot 2^t$，从而

$$1\equiv 2^{\frac{q-1}{2}}\equiv 2^{k\cdot 2^t}=(2^{2^t})^k\equiv(-1)^k \pmod{q}.$$

于是 $1\equiv(-1)^k \pmod{q}$．由于 q 是奇素数，k 必须是偶数：

$$k=2h.$$

证毕．

例如，$F_5=2^{32}+1=641\cdot 6700417$，这时，有

$$2^{t+2}=2^7=128.$$

根据引理 3，F_5 的两个素因子可表作

$$128\cdot h+1$$

的形状. 实际上

$$641=128\cdot 5+1,$$

$$6700417=128\cdot 52347+1.$$

又例如, $F_6=2^{64}+1=274177\cdot 67280421310721,$

这时 $2^{t+2}=2^8=256$. F_6 的两个素因子可表为

$$274177=1071\cdot 256+1,$$

$$67280421310721=262814145745\cdot 256+1.$$

二、Fermat 数变换

1. 当 $1\leqslant t\leqslant 4$, F_t 是素数的情形.

由于 $O(F_t)=2^{2^t}$, 故 N 可取作

$$N=2^m\quad (0<m\leqslant 2^t),\quad N_{\max}=2^{2^t}.$$

N 确定后, 不难确定相应的 α.

1° 当 $N=2b=2^{t+1}$ 时, $\alpha=2$.

这是因为 $\quad 2^{2b}=(2^{2^t})^2\equiv 1\pmod{F_t}$.

$$2^b\equiv 2^{2^t}\equiv -1\pmod{F_t}.$$

2° 当 $N=N_{\max}=2^{2^t}$ 时, $\alpha=3$.

也就是说, $\alpha=3$ 是模 $F_t(1\leqslant t\leqslant 4)$ 的主根. 为要证明 $\alpha=3$ 是模 F_t 的主根, 只需证明

$$3^{\varphi(F_t)}\equiv 1\pmod{F_t},\qquad 3^{\frac{\varphi(F_t)}{2}}\equiv -1\pmod{F_t}.$$

前一式是显然的, 这是因为 $(3, F_t)=1$, 由 Fermat 定理直接得到. 因此只需证明后一式. 因为

$$\left(\frac{3}{F_t}\right)\equiv 3^{\frac{F_t-1}{2}}\pmod{F_t},$$

其中 $\left(\frac{q}{p}\right)$ 是 Legendre 符号(p 是素数)．当 $t\geqslant 1$ 时，

$$F_t=2^{2^t}+1\equiv 1 \pmod 4.$$

故由反转律，有

$$\left(\frac{3}{F_t}\right)=\left(\frac{F_t}{3}\right).$$

但 $F_t-2=2^{2^t}-1=4^{2^{t-1}}-1$ 恒为 3 的倍数，故

$$F_t=2 \pmod 3.$$

于是

$$\left(\frac{3}{F_t}\right)=\left(\frac{F_t}{3}\right)=\left(\frac{2}{3}\right)=-1.$$

因此

$$3^{\frac{\varphi(F_t)}{2}}=3^{\frac{F_t-1}{2}}\equiv\left(\frac{3}{F_t}\right)=-1 \pmod{F_t}.$$

所以 3 是模 $F_t(1\leqslant t\leqslant 4)$ 的主根．证毕．

例 1 当 $t=2$，$F_t=17$．

这时 $O(F_t)=16$，故 N 可取 16 的因子 2, 4, 8, 16($N=1$ 无实际意义)．因为 $\varphi(2)=1$，$\varphi(4)=2$，$\varphi(8)=4$，$\varphi(16)=8$，故相应的 α_N 共有 $1+2+4+8=15$ 个(加上对应于 $N=1$ 的 $\varphi(1)=1$ 个，共 16 个)．N 与 α_N 的值如下表．

表 2 $M=17$

N	α_N
1	1
2	16
4	2, 13
8	2, 8, 9, 15
16	3, 5, 6, 7, 10, 11, 12, 14

2．当 $t\geqslant 5$, $M=F_t=2^b+1$, $b=2^t$ 的情形.

这时 F_t 可能为复合数. 根据引理 2, 可取 $N=2^{t+1}$. 又当 $t\geqslant 2$ 时,根据引理 3, 可取 $N=2^{t+2}$.

1° 可以证明, $N=2^{t+1}$, $\alpha_N=2$*.

由于 $N|O(F_t)$, 故对于 F_t 的任一素因子 p, 有 $(N, p)=1$, 从而 $(N, M)=1$, 即 $(2^{t+1}, 2^{2^t}+1)=1$, 故 N 在 Z_{F_t} 中有逆元 $N^{-1}(N^{-1}=2^{2^{t-1}-(t+1)})$.

又由于 $2^N=2^{2^{t+1}}=(2^{2^t})^2\equiv 1 \pmod{F_t}$,

$$2^{\frac{N}{2}}=2^{2^t}\equiv -1 \pmod{F_t},$$

这表示 2 对模 F_t 的阶数是 2^{t+1}. 再设 p 为 F_t 的任一素因子. 可以证明, 2 对模 p 的阶数是 2^{t+1}. 事实上,设 2 对模 p 的阶数是 d, 由于 $2^{2^{t+1}}\equiv 1 \pmod p$, 故 $d|2^{t+1}$. 不妨设 $d=2^l$, $0<l\leqslant t+1$. 如果 $l<t+1$, 那么由 $2^{2^l}\equiv 1 \pmod p$, 可得到 $[2^{2^l}]^{2^{t-l}}\equiv 1 \pmod p$, 从而得到 $2^{2^t}\equiv +1 \pmod p$, 但这与 $2^{2^t}\equiv -1 \pmod p$ 矛盾. 于是 $l=t+1$, 故 $d=2^l=2^{t+1}$. 这样就证明了 2 对模 p 的阶数是 $2^{t+1}=N$. 因此, 根据 **4** 中定理 1 知, $\{N=2^{t+1}, \alpha_N=2\}$ 满足 NTT 的条件.

2° $t\geqslant 2$ 时, $N=4b=2^{t+2}$, $\alpha_N=\sqrt{2}$.

显然有 $(2^{t+2}, 2^{2^t}+1)=1$, 故 $N=2^{t+2}$ 在 Z_{F_t} 中存在逆元 $N^{-1}(N^{-1}=2^{2^{t+2}-(t+2)})$.

可以证明, $\alpha_N=\sqrt{2}=2^{\frac{b}{4}}(2^{\frac{b}{2}}-1)$ 满足 **4** 中的定理 1 的条件. 事实上,

由于 $\alpha_N^2=2^{\frac{b}{2}}(2^{\frac{b}{2}}-1)^2=2^{\frac{b}{2}}(2^b-2\cdot 2^{\frac{b}{2}}+1)$

$$\equiv -2\cdot 2^b\equiv 2 \pmod{F_t},$$

* 用 **4** 中定理 3 来证明 $\{\alpha=2, N=2^{t+1}\}$ 及 $\{\alpha=\sqrt{2}, N=2^{t+1}\}$ 适合 NTT 的条件, 请参阅 **12**.

故 $\alpha_N^N=\alpha_N^{4b}=(\alpha_N^2)^{2b}\equiv 2^{2b}=(2^b)^2\equiv 1 \pmod{F_t}$,

$$\alpha_N^{\frac{N}{2}}=\alpha_N^{2b}=(\alpha_N^2)^b\equiv 2^b\equiv -1 \pmod{F_t}.$$

这表示 $\alpha_N=\sqrt{2}=2^{\frac{b}{4}}(2^{\frac{b}{2}}-1)$ 对模 F_t 的阶为 $2^{t+2}=N$.

再设 p 是 F_t 的任一素因子，并设 $\alpha_N=\sqrt{2}$ 对模 p 的阶为 d. 由于有

$$\alpha_N^N=[\sqrt{2}]^{2^{t+2}}\equiv 1 \pmod{p},$$

$$\alpha_N^{\frac{N}{2}}=[\sqrt{2}]^{2^{t+1}}\equiv -1 \pmod{p},$$

故 $d|2^{t+2}$. 不妨设 $d=2^l$, $0<l\leqslant t+2$. 如果 $l<t+2$, 那么由 $[\sqrt{2}]^{2^l}\equiv 1 \pmod{p}$, 可得到

$$\{[\sqrt{2}]^{2^l}\}^{2^{t-l+1}}=\{\sqrt{2}\}^{2^{t+1}}\equiv 1 \pmod{p},$$

但这与 $[\sqrt{2}]^{2^{t+1}}\equiv -1 \pmod{p}$ 矛盾，故 $l=t+2$, 即 $d=2^{t+2}=N$. 这就证明了 $\alpha_N=\sqrt{2}$ 对模 p 的阶是 $N=2^{t+2}$. 故 $\{N=2^{t+2}, \alpha_N=\sqrt{2}\}$ 满足 NTT 的条件.

总结1. 和2. 两种情况，将可实现 FNT 的参数 M、N、α 列于表3. 表3还给出了最大可能长度 N_{max} 及相应的 α.

表3 实现 FNT 的参数 M、N、α

t	$b=2^t$	$M=F_t=2^b+1$	N $\alpha=2$	$\alpha=\sqrt{2}$	$\alpha=3$	N_{max}	N_{max} 时 α
1	2	5	4	—	4	4	2, 3
2	4	17	8	16	16	16	$\sqrt{2}$, 3
3	8	257	16	32	256	256	3
4	16	$2^{16}+1$	32	64	2^{16}	2^{16}	3
5	32	$2^{32}+1$	64	128	—	128	$\sqrt{2}$
6	64	$2^{64}+1$	128	256	—	256	$\sqrt{2}$

例 2 设有两个序列

$$\{x_n\}=\begin{bmatrix} x_0\\ x_1\\ x_2\\ x_3 \end{bmatrix}=\begin{bmatrix} 1\\ 0\\ 2\\ -2 \end{bmatrix},\qquad \{h_n\}=\begin{bmatrix} h_0\\ h_1\\ h_2\\ h_3 \end{bmatrix}=\begin{bmatrix} 1\\ -1\\ 0\\ -2 \end{bmatrix},$$

试求其循环卷积.

【解】 由于 $|x_n|_{\max}\sum_{k=0}^{3}|h_k|=2\cdot 4=8,$

故可取 $M=F_2=17$, $N=4$, $\alpha=4$, 变换矩阵 T_4 为

$$T_4\equiv\begin{bmatrix} 1 & 1 & 1 & 1\\ 1 & 4 & 4^2 & 4^3\\ 1 & 4^2 & 4^4 & 4^6\\ 1 & 4^3 & 4^6 & 4^9 \end{bmatrix}\equiv\begin{bmatrix} 1 & 1 & 1 & 1\\ 1 & 4 & -1 & -4\\ 1 & -1 & 1 & -1\\ 1 & -4 & -1 & 4 \end{bmatrix}$$

$$\equiv\begin{bmatrix} 1 & 1 & 1 & 1\\ 1 & 4 & 16 & 13\\ 1 & 16 & 1 & 16\\ 1 & 13 & 16 & 4 \end{bmatrix}\quad(\mathrm{mod}17).$$

由于 $4^{-1}\equiv 13\ (\mathrm{mod}17)$, 故变换 T_4 的逆矩阵 T_4^{-1} 为

$$T_4^{-1}\equiv 13\begin{bmatrix} 1 & 1 & 1 & 1\\ 1 & 4^{-1} & 4^{-2} & 4^{-3}\\ 1 & 4^{-2} & 4^{-4} & 4^{-6}\\ 1 & 4^{-3} & 4^{-6} & 4^{-9} \end{bmatrix}\equiv -4\begin{bmatrix} 1 & 1 & 1 & 1\\ 1 & -4 & -1 & 4\\ 1 & -1 & 1 & -1\\ 1 & 4 & -1 & 4 \end{bmatrix}$$

$$\equiv 13\begin{bmatrix} 1 & 1 & 1 & 1\\ 1 & 13 & 16 & 4\\ 1 & 16 & 1 & 16\\ 1 & 4 & 16 & 4 \end{bmatrix}\quad(\mathrm{mod}17).$$

于是

$$\{X_k\}=\begin{bmatrix}X_0\\X_1\\X_2\\X_3\end{bmatrix}\equiv T_4\begin{bmatrix}x_0\\x_1\\x_2\\x_3\end{bmatrix}$$

$$\equiv\begin{bmatrix}1&1&1&1\\1&4&16&13\\1&16&1&16\\1&13&16&4\end{bmatrix}\begin{bmatrix}1\\0\\2\\15\end{bmatrix}\equiv\begin{bmatrix}1\\7\\5\\8\end{bmatrix}\quad(\mathrm{mod}17).$$

$$\{H_k\}=\begin{bmatrix}H_0\\H_1\\H_2\\H_3\end{bmatrix}\equiv T_4\begin{bmatrix}h_0\\h_1\\h_2\\h_3\end{bmatrix}\equiv\begin{bmatrix}15\\5\\4\\14\end{bmatrix}\quad(\mathrm{mod}17).$$

利用 FNT 的循环卷积特性，有

$$\{Y_k\}=\begin{bmatrix}Y_0\\Y_1\\Y_2\\Y_3\end{bmatrix}=\begin{bmatrix}X_0H_0\\X_1H_1\\X_2H_2\\X_3H_3\end{bmatrix}\equiv\begin{bmatrix}15\\35\\20\\112\end{bmatrix}\equiv\begin{bmatrix}15\\1\\3\\10\end{bmatrix}\quad(\mathrm{mod}17).$$

再求 $\{Y_k\}$ 的逆变换，得

$$\{y_n\}=\begin{bmatrix}y_0\\y_1\\y_2\\y_3\end{bmatrix}\equiv T_4^{-1}\begin{bmatrix}Y_0\\Y_1\\Y_2\\Y_3\end{bmatrix}$$

$$=13\begin{bmatrix}1&1&1&1\\1&13&16&4\\1&16&1&16\\1&4&16&4\end{bmatrix}\begin{bmatrix}15\\1\\3\\10\end{bmatrix}\equiv\begin{bmatrix}3\\12\\6\\11\end{bmatrix}\quad(\mathrm{mod}17).$$

取其绝对最小剩余，得到卷积的真值为

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 3 \\ -5 \\ 6 \\ -6 \end{bmatrix}.$$

对于 FNT 而言，由表 3 知，变换长度 $N=2b=2^{t+1}$ 或者 $N=4b=2^{t+2}$，相应的 $\alpha_{2b}=2$，$\alpha_{4b}=\sqrt{2}$，N 是高度复合数，从而 FNT 具有 FFT 类型的快速算法，$\alpha_{2b}=2$，$\alpha_{4b}=\sqrt{2}$，故作 α 的方幂的乘法时，仅为移位操作（当 $\alpha_{4b}=\sqrt{2}$ 时，乘 α 的偶次方幂的计算很简单，仅为移位操作，乘 α 的奇次方幂时，需要乘一次 $\sqrt{2}$，而 $\sqrt{2}$ 的二进制表示是一个二位数，故计算量比 $\alpha=2$ 时略大些）．由例 2 知，作一个 N 点的循环卷积，需要两个正变换及一个逆变换及 N 次乘法，如果用快速算法，共需 $3N\log_2 N$ 次移位操作，和 $3N\log_2 N$ 次加法以及 N 次乘法，计算量大为节省．因此，将 FNT 用于数字滤波，看来是最有前途的．但是由于字长 $b=2^t$，而变换长度 N 与 b 成正比，这样，可供选择的字长太少，从而限制了选择字长的灵活性；当所需的变换长度 N 较大时，b 也较大，从而增加了实现的复杂性，这两点是 FNT 的主要缺点．利用 **11** 和 **14** 中的方法，可适当加以改善．

—10—

应用 Fermat 数变换计算复数卷积

对于两个长为 N 的实整数序列 $\{x_n\}$ 和 $\{h_n\}$，可以利用 FNT 的循环卷积特性计算它们的循环卷积 $\{y_n\}$:

$$y_n=\sum_{k=0}^{N-1}x_k h_{\langle n-k\rangle_N}\quad (n=0,\ 1,\ \cdots,\ N-1).$$

即有 $$\{y_n\}=\mathrm{IFNT}\{\mathrm{FNT}\{x_n\}\cdot\mathrm{FNT}\{h_n\}\}.$$

这种方法所需要的计算量是两个正变换，一个逆变换，N 个乘法及若干个加法.

如果从数字滤波角度看，$\{x_n\}$ 为滤波器输入信号序列，$\{h_n\}$ 为滤波器的单位脉冲响应序列，$\{y_n\}$ 则为输出信号序列. 但是在雷达、声纳(Sonar)等许多应用中不能忽视信号的相位信息，输入信号实际上是一个复信号. $\{h_n\}$ 也是一个复序列. 在这种情况下，如何用 FNT 求它们的复数卷积，这是本节叙述的一个问题. 另一个将叙述的问题是，如果应用复整数序列(所谓复整数，意指其实部和虚部均为整数的复数)在整数环 Z_M 上的特殊表示法，那么可以得到计算复数卷积的一个一般公式，从而能够节省计算量.

一、Fermat 数环(域)中的复数卷积

设两个长为 N 的复整数序列 $\{x_n\}$，$\{y_n\}$ $(n=0,\ 1,\ \cdots,\ N-1)$，其循环卷积仍定义为

$$y_n=\sum_{k=0}^{N-1}x_k h_{\langle n-k\rangle_N}\quad (n=0,\ 1,\ \cdots,\ N-1).\qquad (1)$$

令

$$\left.\begin{aligned} x_n &= \hat{x}_n + j\hat{\hat{x}}_n \\ h_n &= \hat{h}_n + j\hat{\hat{h}}_n \\ y_n &= \hat{u}_n + j\hat{\hat{u}}_n \end{aligned}\right\} \quad j=\sqrt{-1}, \tag{2}$$

那么 $\hat{u}_n$ 和 $\hat{\hat{u}}_n$ 为:

$$\hat{u}_n = \sum_{k=1}^{N-1} (\hat{x}_k \hat{h}_{\langle n-k\rangle_N} - \hat{\hat{x}}_k \hat{\hat{h}}_{\langle n-k\rangle_N}), \tag{3}$$

$$\hat{\hat{u}}_n = \sum_{k=0}^{N-1} (\hat{x}_k \hat{\hat{h}}_{\langle n-k\rangle_N} + \hat{\hat{x}}_k \hat{h}_{\langle n-k\rangle_N}). \tag{4}$$

由(3)和(4)知，直接计算每一个输出值 y_n，需要 $4N$ 个乘法和 $4N-2$ 个加法. 计算出所有的 y_n，共需 $4N^2$ 个乘法及 $4N^2-2N$ 个加法.

现在在 Fermat 数环 Z_{F_t} 中计算卷积.

按下式

$$\max\left\{|\hat{x}_n|_{\max}\sum_{k=0}^{N-1}|\hat{h}_k|,\ |\hat{x}_n|_{\max}\sum_{k=0}^{N-1}|\hat{\hat{h}}_k|,\ |\hat{\hat{x}}_n|_{\max}\sum_{k=0}^{N-1}|\hat{h}_k|,\ |\hat{\hat{x}}_n|_{\max}\sum_{k=0}^{N-1}|\hat{\hat{h}}_k|\right\}<\frac{M}{2} \quad (n=0,\ 1,\ \cdots,\ N-1)$$

选取模 $M=F_t$.

由于 $M=F_t=2^b+1$，$b=2^t$，故

$$2^b \equiv -1 \pmod{F_t},$$

从而有

$$2^{\frac{b}{2}} \equiv \sqrt{-1} = j \pmod{F_t}.$$

因此可将(2)式写作

$$\left.\begin{aligned} x_n &\equiv \hat{x}_n + 2^{\frac{b}{2}}\hat{\hat{x}}_n \\ h_n &\equiv \hat{h}_n + 2^{\frac{b}{2}}\hat{\hat{h}}_n \\ y_n &\equiv \hat{u}_n + 2^{\frac{b}{2}}\hat{\hat{u}}_n \end{aligned}\right\} \pmod{F_t}. \tag{5}$$

于是

$$y_n \equiv \sum_{k=0}^{N-1} (\hat{x}_k + 2^{\frac{b}{2}} \hat{\hat{x}}_k)(\hat{h}_{\langle n-k\rangle_N} + 2^{\frac{b}{2}} \hat{\hat{h}}_{\langle n-k\rangle_N}) \quad (\mathrm{mod} F_t). \tag{6}$$

(5)式表示，一个复整数可与 Z_{F_t} 内的一个整数同余，但是，看来还找不到一个复整数与 Z_{F_t} 内的已知整数同余. 为了解决这矛盾，引进一个辅助卷积 z_n:

$$z_n \equiv \sum_{k=0}^{N-1} (\hat{x}_k - 2^{\frac{b}{2}} \hat{\hat{x}}_k)(\hat{h}_{\langle n-k\rangle_N} - 2^{\frac{b}{2}} \hat{\hat{h}}_{\langle n-k\rangle_N}) \quad (\mathrm{mod} F_t), \tag{7}$$

亦即

$$z_n \equiv \hat{u}_n - 2^{\frac{b}{2}} \hat{\hat{u}}_n \quad (\mathrm{mod} F_t). \tag{8}$$

于是由(5)和(8)，就得到 $\hat{u}_n$ 和 $\hat{\hat{u}}_n$ 为:

$$\left.\begin{aligned} 2\hat{u}_n &\equiv y_n + z_n \\ 2\cdot 2^{\frac{b}{2}} \hat{\hat{u}}_n &\equiv y_n - z_n \end{aligned}\right\} (\mathrm{mod} F_t).$$

由于

$$2\cdot(-2^{b-1}) \equiv 1 \ (\mathrm{mod} F_t), \quad 2^{\frac{b+2}{2}}(-2^{\frac{b-2}{2}}) \equiv 1 \ (\mathrm{mod} F_t),$$

这样有

$$2^{-1} \equiv -2^{b-1} (\mathrm{mod} F_t),$$

$$(2^{\frac{b+2}{2}})^{-1} \equiv -2^{\frac{b-2}{2}} \quad (\mathrm{mod} F_t).$$

所以得到:

$$\hat{u}_n \equiv -2^{b-1}(y_n + z_n) \quad (\mathrm{mod} F_t), \tag{9}$$

$$\hat{\hat{u}}_n \equiv -2^{\frac{b-2}{2}}(y_n - z_n) \quad (\mathrm{mod} F_t), \tag{10}$$

其中 y_n 和 z_n 分别由(6)和(7)所示.

这样计算出 $\hat{u}_n$ 和 $\hat{\hat{u}}_n$ 后，再取其绝对最小剩余，就得到 $\hat{u}_n$ 和 $\hat{\hat{u}}_n$ 的真值，从而得到 y_n 的真值. 从(6)、(7)、(9)、(10)可知，计算一个 y_n（即一个 $\hat{u}_n$ 和一个 $\hat{\hat{u}}_n$）只需要 $2N$ 个乘法及 $2N+4$ 个加法，与一般方法比较，计算量节省了一半. 然而，这里的乘法和加法必须在整数环 Z_{F_t} 内进行.

二、应用 Fermat 数变换计算复数卷积

记

$$
\begin{aligned}
\hat{X}_k &= \mathrm{FNT}\{\hat{x}_n\},\\
\hat{\hat{X}}_k &= \mathrm{FNT}\{\hat{\hat{x}}_n\},\\
\hat{H}_k &= \mathrm{FNT}\{\hat{h}_n\},\\
\hat{\hat{H}}_k &= \mathrm{FNT}\{\hat{\hat{h}}_n\},\\
\hat{U}_k &= \mathrm{FNT}\{\hat{u}_n\},\\
\hat{\hat{U}}_k &= \mathrm{FNT}\{\hat{\hat{u}}_n\}.
\end{aligned}
\tag{11}
$$

于是，由(3)和(4)就得到

$$\hat{U}_k = \hat{X}_k\hat{H}_k - \hat{\hat{X}}_k\hat{\hat{H}}_k, \tag{12}$$

$$\hat{\hat{U}}_k = \hat{X}_k\hat{\hat{H}}_k + \hat{\hat{X}}_k\hat{H}_k. \tag{13}$$

再应用逆变换，就得到

$$\hat{u}_n \equiv \mathrm{IFNT}\{\hat{U}_k\} = \mathrm{IFNT}\{\hat{X}_k\hat{H}_k - \hat{\hat{X}}_k\hat{\hat{H}}_k\}, \tag{14}$$

$$\hat{\hat{u}}_n \equiv \mathrm{IFNT}\{\hat{\hat{U}}_k\} = \mathrm{IFNT}\{\hat{X}_k\hat{\hat{H}}_k + \hat{\hat{X}}_k\hat{H}_k\}. \tag{15}$$

应用这个方法，对于 N 点的复数循环卷积，所需要的计算量是六个变换(四个正变换，两个逆变换)，$4N$ 个乘法及 $2N$ 个加法.

如果应用(9)和(10)式，那么

$$
\begin{aligned}
\hat{U}_k \equiv -2^{b-1}\{&(\hat{X}_k + 2^{\frac{b}{2}}\hat{\hat{X}}_k)(\hat{H}_k + 2^{\frac{b}{2}}\hat{\hat{H}}_k)\\
&+ (\hat{X}_k - 2^{\frac{b}{2}}\hat{\hat{X}}_k)(\hat{H}_k - 2^{\frac{b}{2}}\hat{\hat{H}}_k)\} \pmod{F_t},
\end{aligned}
\tag{16}
$$

$$
\begin{aligned}
\hat{\hat{U}}_k \equiv -2^{\frac{b-2}{2}}\{&(\hat{X}_k + 2^{\frac{b}{2}}\hat{\hat{X}}_k)(\hat{H}_k + 2^{\frac{b}{2}}\hat{\hat{H}}_k)\\
&- (\hat{X}_k - 2^{\frac{b}{2}}\hat{\hat{X}}_k)(\hat{H}_k - 2^{\frac{b}{2}}\hat{\hat{H}}_k)\} \pmod{F_t}.
\end{aligned}
\tag{17}
$$

应用逆变换，就得到

$$\hat{u}_n \equiv -2^{b-1}\mathrm{IFNT}\{(\hat{X}_k+2^{\frac{b}{2}}\hat{\hat{X}}_k)(\hat{H}_k+2^{\frac{b}{2}}\hat{\hat{H}}_k)$$
$$+(\hat{X}_k-2^{\frac{b}{2}}\hat{\hat{X}}_k)(\hat{H}_k-2^{\frac{b}{2}}\hat{\hat{H}}_k)\} \quad (\mathrm{mod}F_t), \qquad (18)$$

$$\hat{\hat{u}}_n \equiv -2^{\frac{b-2}{2}}\mathrm{IFNT}\{(\hat{X}_k+2^{\frac{b}{2}}\hat{\hat{X}}_k)(\hat{H}_k+2^{\frac{b}{2}}\hat{\hat{H}}_k)$$
$$-(\hat{X}_k-2^{\frac{b}{2}}\hat{\hat{X}}_k)(\hat{H}_k-2^{\frac{b}{2}}\hat{\hat{H}}_k)\} \quad (\mathrm{mod}F_t). \qquad (19)$$

(18)、(19)与(14)、(15)比较，两者均需要六个变换，但这里只需要 $2N$ 个乘法及 $6N$ 个加法，所需的乘法减少一半。

例 设两个复整数序列为

$$\left.\begin{aligned} x_n &= \hat{x}_n + j\hat{\hat{x}}_n \\ h_n &= \hat{h}_n + j\hat{\hat{h}}_n \end{aligned}\right\} \quad (n=0,\ 1,\ 2,\ \cdots,\ N-1),$$

其中，
$$(\hat{x}) = \{\hat{x}_n\} = \begin{bmatrix} \hat{x}_0 \\ \hat{x}_1 \\ \hat{x}_2 \\ \hat{x}_3 \end{bmatrix} = \begin{bmatrix} 2 \\ -2 \\ 1 \\ 0 \end{bmatrix},$$

$$(\hat{\hat{x}}) = \{\hat{\hat{x}}_n\} = \begin{bmatrix} \hat{\hat{x}}_0 \\ \hat{\hat{x}}_1 \\ \hat{\hat{x}}_2 \\ \hat{\hat{x}}_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 2 \\ -2 \end{bmatrix},$$

$$(\hat{h}) = \{\hat{h}_n\} = \begin{bmatrix} \hat{h}_0 \\ \hat{h}_1 \\ \hat{h}_2 \\ \hat{h}_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 0 \\ 0 \end{bmatrix},$$

$$(\hat{\hat{h}}) = \{\hat{\hat{h}}_n\} = \begin{bmatrix} \hat{\hat{h}}_0 \\ \hat{\hat{h}}_1 \\ \hat{\hat{h}}_2 \\ \hat{\hat{h}}_3 \end{bmatrix} = \begin{bmatrix} 1 \\ -1 \\ 0 \\ -2 \end{bmatrix}.$$

试计算它们的循环卷积

$$y_n = \sum_{k=0}^{3} x_k h_{\langle n-k \rangle_4} \quad (n=0,\ 1,\ 2,\ 3).$$

【解】 由于

$$\max\left\{ |\hat{x}_n|_{\max} \sum_{k=0}^{3} |\hat{h}_k|,\quad |\hat{x}_n|_{\max} \sum_{k=0}^{3} |\hat{\hat{h}}_k|,\quad |\hat{\hat{x}}_n|_{\max} \sum_{k=0}^{3} |\hat{h}_k|,\right.$$

$$\left. |\hat{\hat{x}}_n|_{\max} \sum_{k=0}^{3} |\hat{\hat{h}}_k| \right\} = 8,$$

故取 $M = F_2 = 17,\quad N = 4,\quad \alpha = 4,$

$$T_4 \equiv \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 4 & -1 & -4 \\ 1 & -1 & 1 & -1 \\ 1 & -4 & -1 & 4 \end{bmatrix} \pmod{17},$$

$$T_4^{-1} \equiv -4 \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -4 & -1 & 4 \\ 1 & -1 & 1 & -1 \\ 1 & 4 & -1 & 4 \end{bmatrix} \pmod{17}.$$

于是，$$(\hat{X}) \equiv T_4(\hat{x}) \equiv \begin{bmatrix} 1 \\ 10 \\ 5 \\ 9 \end{bmatrix} \pmod{17},$$

$$(\hat{\hat{X}}) \equiv T_4(\hat{\hat{x}}) \equiv \begin{bmatrix} 1 \\ 7 \\ 5 \\ 8 \end{bmatrix} \pmod{17},$$

$$(\hat{H}) \equiv T_4(\hat{h}) \equiv \begin{bmatrix} 3 \\ 9 \\ 16 \\ 10 \end{bmatrix} \pmod{17},$$

$$(\hat{\hat{H}}) \equiv T_4(\hat{\hat{h}}) \equiv \begin{bmatrix} 15 \\ 5 \\ 4 \\ 14 \end{bmatrix} \pmod{17}.$$

根据(12)和(13),有

$$(\hat{U}) \equiv \{\hat{X}_k \hat{H}_k - \hat{\hat{X}}_k \hat{\hat{H}}_k\} \equiv \begin{bmatrix} 5 \\ 4 \\ 9 \\ -5 \end{bmatrix} \pmod{17},$$

$$(\hat{\hat{U}}) \equiv \{\hat{X}_k \hat{\hat{H}}_k + \hat{\hat{X}}_k \hat{H}_k\} \equiv \begin{bmatrix} 1 \\ -6 \\ -2 \\ 2 \end{bmatrix} \pmod{17}.$$

应用逆变换,就得到:

$$(\hat{u}) = \mathrm{IFNT}(\hat{U}) \equiv T_4^{-1} \begin{bmatrix} 5 \\ 4 \\ 9 \\ -5 \end{bmatrix} \equiv \begin{bmatrix} -1 \\ 7 \\ 8 \\ 8 \end{bmatrix} \pmod{17},$$

$$(\hat{\hat{u}}) = \mathrm{IFNT}(\hat{\hat{U}}) \equiv T_4^{-1} \begin{bmatrix} 1 \\ -6 \\ -2 \\ 2 \end{bmatrix} \equiv \begin{bmatrix} 3 \\ -4 \\ 5 \\ 1 \end{bmatrix} \pmod{17}.$$

取其绝对最小剩余，得

$$(\hat{u})=\begin{bmatrix}-1\\7\\8\\8\end{bmatrix},\qquad(\hat{\hat{u}})=\begin{bmatrix}3\\-4\\5\\1\end{bmatrix}.$$

于是由 $(y)=(\hat{u})+j(\hat{\hat{u}})$，得到

$$(y)=\begin{bmatrix}y_0\\y_1\\y_2\\y_3\end{bmatrix}=\begin{bmatrix}-1+j3\\7-j4\\8+j5\\8+j\end{bmatrix}.$$

这就是用一般 FNT 算法算出的所给复整数序列的卷积值.

如果应用(18)和(19)式，那么

$$j\equiv2^{\frac{b}{2}}\equiv4\pmod{17}.$$

于是由(16)和(17)，得到

$$(\hat{U})=\begin{bmatrix}\hat{U}_0\\\hat{U}_1\\\hat{U}_2\\\hat{U}_3\end{bmatrix}$$

$$\equiv-2^3\begin{bmatrix}(\hat{X}_0+4\hat{\hat{X}}_0)(\hat{H}_0+4\hat{\hat{H}}_0)+(\hat{X}_0-4\hat{\hat{X}}_0)(\hat{H}_0-4\hat{\hat{H}}_0)\\(\hat{X}_1+4\hat{\hat{X}}_1)(\hat{H}_1+4\hat{\hat{H}}_1)+(\hat{X}_1-4\hat{\hat{X}}_1)(\hat{H}_1-4\hat{\hat{H}}_1)\\(\hat{X}_2+4\hat{\hat{X}}_2)(\hat{H}_2+4\hat{\hat{H}}_2)+(\hat{X}_2-4\hat{\hat{X}}_2)(\hat{H}_2-4\hat{\hat{H}}_2)\\(\hat{X}_3+4\hat{\hat{X}}_3)(\hat{H}_3+4\hat{\hat{H}}_3)+(\hat{X}_3-4\hat{\hat{X}}_3)(\hat{H}_3-4\hat{\hat{H}}_3)\end{bmatrix}$$

$$\equiv-8\begin{bmatrix}-25+18\\-20-6\\-16\\-14-30\end{bmatrix}\equiv\begin{bmatrix}5\\4\\9\\-5\end{bmatrix}\pmod{17},$$

$$(\hat{U})=\begin{bmatrix}\hat{U}_0\\\hat{U}_1\\\hat{U}_2\\\hat{U}_3\end{bmatrix}\equiv-2\begin{bmatrix}-25-18\\-20+6\\-16\\-14+30\end{bmatrix}\equiv\begin{bmatrix}1\\-6\\-2\\2\end{bmatrix}\pmod{17}.$$

利用逆变换，得

$$(\hat{u})=\mathrm{IFNT}(\hat{U})=T_4^{-1}(\hat{U})\equiv\begin{bmatrix}-1\\7\\8\\8\end{bmatrix}\pmod{17},$$

$$(\hat{\hat{u}})=\mathrm{IFNT}(\hat{\hat{U}})=T_4^{-1}(\hat{\hat{U}})\equiv\begin{bmatrix}3\\-4\\5\\1\end{bmatrix}\pmod{17}.$$

取其绝对最小剩余，得

$$(\hat{u})=\begin{bmatrix}-1\\7\\8\\8\end{bmatrix},\qquad(\hat{\hat{u}})=\begin{bmatrix}3\\-4\\5\\1\end{bmatrix}.$$

于是所求卷积值为

$$(y)=\begin{bmatrix}y_0\\y_1\\y_2\\y_3\end{bmatrix}=\begin{bmatrix}-1+j3\\7-j4\\8+j5\\8+j\end{bmatrix}.$$

从上例知，用本节的方法(即利用(18)和(19)两式)计算复数

卷积，比一般方法(即(14)和(15)两式)所需乘法次数减少一半．而且，这两种方法都是在同一整数环 Z_M 内进行运算的．这就是说，本节的方法，是在不增加字长的情况下，使乘法次数减少一半．但是，如果按如下步骤进行计算：

$$(y)=\{y_n\}=\mathrm{IFNT}\{\mathrm{FNT}\{\hat{x}_n+2^{\frac{b}{2}}\hat{\hat{x}}_n\}\cdot\mathrm{FNT}\{\hat{h}_n+2^{\frac{b}{2}}\hat{\hat{h}}_n\}\},$$

$$(z)=\{z_n\}=\mathrm{IFNT}\{\mathrm{FNT}\{\hat{x}_n-2^{\frac{b}{2}}\hat{\hat{x}}_n\}\cdot\mathrm{FNT}\{\hat{h}_n-2^{\frac{b}{2}}\hat{\hat{h}}_n\}\},$$

再由(9)和(10)得出 $\hat{u}_n$ 和 $\hat{\hat{u}}_n$，那么计算量虽亦可比一般方法有所减少，但字长将比一般方法有所增加．

—11—

伪 Fermat 数变换

9 中已经指出，Fermat 数变换的一个主要缺点是字长 b 与变换长度之间存在严格的关系．从表 3 可知，当 $\alpha=2$ 时，$N=2b$；当 $\alpha=\sqrt{2}$ 时，$N=4b$；$b=2^t$．由于 b 随 t 增大极快，所以可供选择的字长极为有限．当需要的字长不是 2 的幂，例如需要的字长是 24，如果取下一个 b，如 $b=32$，那将导致计算的极大浪费．

本节提出两个办法加以改善．

一、在 $M=2^b+1, b=s\cdot 2^t$ 为模的整数环 Z_M 上的变换

取 $M=2^b+1$，$b=s\cdot 2^t$（s 是奇整数，$t=1, 2, \cdots$）作为模，这时

$$2^{2^t}+1 \mid 2^{s\cdot 2^t}+1.$$

所以变换长度 N 决定于 $2^{2^t}+1=F_t$．由 **9** 中引理 2 与引理 3，可取变换长度 $N=2^{t+1}$ 及 $N=2^{t+2}$．

当 $N=2^{t+1}$ 时，$\alpha=2^s$．这是因为

$$\alpha^N=(2^s)^{2^{t+1}}\equiv(2^{s\cdot 2^t})^2\equiv(-1)^2\equiv 1 \pmod{M},$$

$$\alpha^{\frac{N}{2}}=(2^s)^{2^t}\equiv 2^{s\cdot 2^t}\equiv -1 \pmod{M},$$

这表示 $\alpha=2^s$ 对模 M 的阶是 $N=2^{t+1}$．再设 M 的任一素因子是 q，由于有

$$\alpha^N = 2^{s\cdot 2^{t+1}} \equiv 1 \pmod{q},$$

$$\alpha^{\frac{N}{2}} = 2^{s\cdot 2^t} \equiv -1 \pmod{q},$$

所以如设 $\alpha=2^s$ 对模 q 的阶是 d, 那么 $d|2^{t+1}$. 不妨设 $d=2^l$, 于是 $0<l\leqslant t+1$. 如果 $l<t+1$, 那么由于

$$(2^s)^d = (2^s)^{2^l} \equiv 1 \pmod{q},$$

故有 $$[(2^s)^{2^l}]^{2^{t-l}} \equiv (2^s)^{2^t} \equiv 1 \pmod{q}.$$

但这与 $2^{s\cdot 2^t}\equiv -1 \pmod{q}$ 矛盾, 故 $l=t+1$, 即 $d=2^{t+1}$, 这表示 $\alpha=2^s$ 对模 q 的阶是 2^{t+1}. 由于 q 是 M 的任一素因子, 因此, $\alpha=2^s$ 对 M 的所有素因子的阶都是 2^{t+1}. 所以根据 **4** 中定理 1 知, $\{\alpha=2^s,\ N=2^{t+1}\}$ 满足 NTT 的条件. N 与 M 互素是显然的, 故如下变换成立: 设 $x_n\in Z_M(N=0, 1, \cdots, N-1)$, $M=2^b+1$, $b=s\cdot 2^t$, s 为奇整数, 则

$$X_k \equiv \sum_{n=0}^{N-1} x_n 2^{snk} \quad (k=0,\ 1,\ \cdots,\ N-1) \quad (\mathrm{mod} M), \tag{1}$$

$$x_n \equiv N^{-1}\sum_{k=0}^{N-1} X_k 2^{-snk} \quad (n=0,\ 1,\ \cdots,\ N-1)(\mathrm{mod} M), \tag{2}$$

其中 $N=2^{t+1}$.

当 $N=2^{t+2}$ 时, $\alpha=(2^s)^{\frac{1}{2}}=\sqrt{2^s}\quad (t\geqslant 2)$.

这里 $$\alpha=(2^s)^{\frac{1}{2}}=2^{\left(\frac{s-1}{2}+s\cdot 2^{t-2}\right)}[2^{s\cdot 2^{t-1}}-1].$$

首先,
$$\begin{aligned}\alpha^2 &= 2^{\left(\frac{s-1}{2}+s\cdot 2^{t-2}\right)\cdot 2}[2^{s\cdot 2^{t-1}}-1]^2\\ &= 2^{(s-1+s\cdot 2^{t-1})}(2^{s\cdot 2^t}-2^{s\cdot 2^{t-1}+1}+1)\\ &\equiv -2^{s+s\cdot 2^t}\equiv 2^s \pmod{M},\end{aligned}$$

$$\alpha^N = [(2^s)^{\frac{1}{2}}]^{2^{t+2}} \equiv (2^s)^{2^{t+1}} \equiv 1 \pmod{M},$$

$$\alpha^{\frac{N}{2}} \equiv (2^s)^{2^t} \equiv -1 \pmod{M}.$$

这表示 $\alpha=(2^s)^{\frac{1}{2}}$对模 M 的阶是 $N=2^{t+2}$. 再设 q 是 M 的任

一素因子，且设 $\alpha=(2^s)^{\frac{1}{2}}$ 对模 q 的阶是 d，可以证明 $d=2^{t+2}$. 事实上，由于

$$(\sqrt{2^s})^{2^{t+2}}\equiv 1 \pmod{q}, \quad (\sqrt{2^s})^{2^{t+1}}\equiv -1 \pmod{q},$$

故 $d|2^{t+2}$. 如设 $d=2^l$，于是 $0<l\leqslant t+2$，如果 $l<t+2$，那么由于 $(\sqrt{2^s})^d=(\sqrt{2^s})^{2^l}\equiv 1 (\bmod q)$，所以

$$[(\sqrt{2^s})^{2^l}]^{2^{t+1-l}}\equiv 1 \pmod{q}.$$

也就是 $(\sqrt{2^s})^{2^{t+1}}\equiv 1 (\bmod q)$，但这与 $(\sqrt{2^s})^{2^{t+1}}\equiv -1 (\bmod q)$ 矛盾，所以 $d=2^{t+2}$. 由于 q 是 M 的任一素因子，这表示 $\{\alpha=\sqrt{2^s},\ N=2^{t+2}\}$ 满足 NTT 的条件. 即如下变换成立：

设 $x_n\in Z_M (n=0, 1, \cdots, N-1)$，$M=2^b+1$，$b=s\cdot 2^t$，$s$ 是奇整数，则

$$X_k\equiv\sum_{n=0}^{N-1} x_n(\sqrt{2^s})^{nk} (\bmod M) \quad (k=0, 1, \cdots, N-1), \tag{3}$$

$$x_n\equiv N^{-1}\sum_{k=0}^{N-1} X_k(\sqrt{2^s})^{-nk} (\bmod M) \quad (n=0, 1, \cdots, N-1), \tag{4}$$

其中，$N=2^{t+2}$，$\sqrt{2^s}=2^{\left(\frac{s-1}{2}+s\cdot 2^{t-2}\right)}[2^{s\cdot 2^{t-1}}-1]$. 注意这里 $\sqrt{2^s}$ 是正整数，如 $s=3$，$t=3$ 时，$M=2^{24}+1$，$N=32$，

$$\alpha=\sqrt{2^3}=2^7(2^{10}-1).$$

表 4 列出了在 $Z_M(M=2^b+1, b=s\cdot 2^t, s$ 为奇整数，$t=1, 2, \cdots)$ 上的 NTT 的各种参数. 从表 4 可以看出，字长 b 的选择比较灵活. 但与 FNT 比较，在相同字长的情况下，可实现的变换长度却要短些. 例如，$N=16$，FNT 只需要 $b=8$ 或 4，这里却需要 $b=24$ 或 12. 因此，这种变换的实际意义并不大，在实际应用上似乎只对 $b=24$，40，48 才感兴趣. 但是这种变换的变换长度 N 是 2 的幂，根 α 是 2 的幂，因此具有快速算法及只需移位操作的特点.

这种变换，由于 b 是偶数，亦可用于复数卷积的计算.

在以 $M=2^b+1(b=s\cdot 2^t)$ 为模的整数环 Z_M 上，也可能存在长度大于 2^{t+2} 的变换．例如 $M=2^{40}+1=2^{5\cdot 2^3}+1$，由于 $2^{2^3}+1|2^{40}+1$，故 $N_{\max}=2^{2^3}=256$．又例如 $M=2^{80}+1$，$2^{2^4}+1|2^{80}+1$，故 $N_{\max}=2^{16}=66536$．但是相应的 α 可能不简单．

表 4　在整数环 $Z_M(M=2^b+1, b=s\cdot 2^t, s$ 是奇整数)上的 NTT 的各种参数

s	t	$b=s\cdot 2^t$	$M=2^b+1$	N	
				$\alpha=2^s$	$\alpha=\sqrt{2^s}$
3	1	6	2^6+1	4	—
5	1	10	$2^{10}+1$	4	—
3	2	12	$2^{12}+1$	8	16
7	1	14	$2^{14}+1$	4	—
5	2	20	$2^{20}+1$	8	16
3	3	24	$2^{24}+1$	16	32
7	2	28	$2^{28}+1$	8	16
5	3	40	$2^{40}+1$	16	32
3	4	48	$2^{48}+1$	32	64
7	3	56	$2^{56}+1$	16	32
5	4	80	$2^{80}+1$	32	64

其中 $\sqrt{2^s}=2^{\left(\frac{s-1}{2}+s\cdot 2^{t-2}\right)}[2^{s\cdot 2^{t-1}}-1]\quad(t\geqslant 2)$．

二、伪 Fermat 数变换

如何保持上述变换的优点而使变换长度增加呢？

我们根据 4 中定理 4 来分析一下变换长度受限制的原因．

设 $M=2^b+1$，当 $b\neq 2^t$ 时，M 就不是素数，设可以分解为

$$M=M_1\cdot M_2=\overbrace{p_1^{l_1}\cdots p_r^{l_r}}^{M_1}\cdot\overbrace{p_{r+1}^{l_{r+1}}\cdots p_s^{l_s}}^{M_2},$$

记 $O(M_1)=(p_1-1,\ p_2-1,\ \cdots,\ p_r-1)$,

$O(M_2)=(p_{r+1}-1,\ \cdots,\ p_s-1)$,

由于 $O(M)=(p_1-1,\ \cdots,\ p_r-1,\ p_{r+1}-1,\ \cdots,\ p_s-1)$,

所以有 $O(M)=(O(M_1),\ O(M_2))$.

由**4**中定理 4,变换长度 N 必须是 $O(M)$ 的约数,所以 N 必须是 $O(M_1)$ 和 $O(M_2)$ 的公约数. 可能有这样的情况, M_1 很小, 从而 $O(M_1)$ 很小, 而 $O(M_2)\gg O(M_1)$, 这样 $O(M_2)\gg O(M)$. 在这种情况下,就因为有因子 M_1 而使得变换长度大大减少. 例如

$$M=2^{12}+1=4097=17\cdot 241,$$

$$O(M)=(16,\ 240)=16,$$

$$O(M_1)=16,$$

$$O(M_2)=240$$

就是这种情况. 在 Z_M 上, $N_{max}=16$, 但是以

$$M_2=241=\frac{2^{12}+1}{17}$$

为模的整数环 Z_{M_2} 上, $N_{max}=240$. 也就是说, 在 Z_M 上, 因为有因子 M_1, 只能产生最大变换长度为 16 的 NTT, 而在 Z_{M_2} 上却可以产生最大变换长度为 240 的 NTT. 同时, 以 M_2 为模计算循环卷积 y_n 时, 最大输出范围 $|y_n|_{max}<\frac{M_2}{2}$, 而以 M 为模计算 y_n 时, 最大输出范围 $|y_n|_{max}<\frac{M}{2}$, 因此, 输出范围减少了. 如果有这样的情况, 即由于 M_1 的存在, 使得 N_{max} 大为减少, 同时 M_1 又不能有效地增加最大的允许输出, 即"有效字长", 那么在这样的情况下, 我们可以在以 $M_2=\frac{M}{M_1}$

为模的整数环 Z_{M_2} 上定义 NTT，以减少最大输出的范围为代价来获得变换长度的增加．当 $M=2^b+1(b\neq 2^t)$，这种在 M 的因子 M_2 为模的整数环 Z_{M_2} 上定义的 NTT 叫做伪 Fermat 数变换(Pseudo FNT)．

设 $M=2^b+1(b\neq 2^t)$，其分解式是

$$M=p_1^{l_1}\cdot p_2^{l_2}\cdots p_s^{l_s}.$$

取 $M_2=\dfrac{M}{p_s^{l_s}}$ 为模，如果 $\left\{\alpha=2^w,\quad N=\dfrac{2b}{w}\right\}$满足 NTT 的条件，那么如下变换

$$X_k\equiv\sum_{n=0}^{N-1}x_n 2^{wnk}\quad\left(\bmod\frac{M}{p_s^{l_s}}\right)\quad(k=0,\ 1,\ \cdots,\ N-1),\tag{5}$$

$$x_n\equiv N^{-1}\sum_{k=0}^{N-1}X_k 2^{-wnk}\quad\left(\bmod\frac{M}{p_s^{l_s}}\right)\quad(n=0,\ 1,\ \cdots,\ N-1)\tag{6}$$

称为伪 FNT*．其中，

$$N=\frac{2b}{w},\quad x_n\in Z_{M_2}(n=0,\ 1,\ \cdots,\ N-1).$$

伪 FNT 中的 b 可以是奇整数，也可以是偶整数．对伪 FNT 来说，最要紧的是选择模 M_2．通常取 M 被它的最小因子相除，其商作为模 M_2，以便使 M_2 足以取 $\alpha=2$ 或 $\alpha=\sqrt{2}$ 作为根来定义一个尽可能长的变换．

表 5 列出了当 b 是偶数时，伪 FNT 的各种参数．表中 $\log_2 M_2$ 是有效字长，对表中所列的 M_2 来说，2 对模 M_2 的阶数是 $2b$，同时也列出了有 $\alpha=\sqrt{2}$ 为根的情况，这时 $N=4b$ (b 必须为 4 的倍数)．从表中可以看出，字长的选择比较灵活，当有效字长为 16 时，至少给出 $N=40$ 的变换，最大可给出 $N=96$ 的变换(注意，这里都是指根 α 是 2 或$\sqrt{2}$的情况)，

* 我们只限于根是 $\alpha=2^w$ 的情况，当 α 为其它值时，暂不讨论．

表 5　当 b 是偶数时，在 $Z_{M_2}(M_2=2^b+1/p_s^{l_s})$ 上的伪 FNT 的各种参数

b	$M=2^b+1$ 的分解式 $M=p_1^{l_1}\cdot p_2^{l_2}\cdots p_s^{l_s}$	$O(M)$	M_1	M_2	有效字长 $\log_2 M_2$（约）	$N_{max}=O(M_2)$	在 Z_{M_2} 中 $(\alpha=2)$ $N=2b$	$(\alpha=\sqrt{2})$ $N=4b$
12	17·241	16	17	$2^{12}+1/17$	8	240	24	48
20	17·61681	16	17	$2^{20}+1/17$	16	61680	40	80
22	5·397·2113	4	5	$2^{22}+1/5$	19	132	44	—
24	97·257·673	32	257	$2^{24}+1/257$	16	96	48	96
26	5·53·157·1613	4	5	$2^{26}+1/5$	24	52	52	—
28	17·15790321	16	17	$2^{28}+1/17$	24	15790320	56	112
34	5·137·953·26317	4	5	$2^{34}+1/5$	32	68	68	—
36	17·241·433·38737	16	17·241	$2^{36}+1/17\cdot241$	24	144	72	144
38	5·229·457·525313	4	5	$2^{38}+1/5$	36	76	76	—
40	257·4278255361	256	257	$2^{40}+1/257$	32	4278255360	80	160
44	17·353·2931542417	16	17	$2^{44}+1/17$	40	176	88	—
46	5·277·1013·1657·30269	4	5	$2^{46}+1/5$	44	92	92	—
48	193·65537·22253377	64	65537	$2^{48}+1/65537$	32	192	96	192
56	257·5153·54410972897	32	257	$2^{56}+1/257$	48	224	112	224
60	17·241·61681·4562284561	16	17·241·61681	$2^{60}+1/17\cdot241\cdot61681$	32	4562284560	120	240
72	97·257·673·577·487824887233	32	97·257·673	$2^{72}+1/97\cdot257\cdot673$	48	576	144	288
80	65537·414721·44479210368001	1024	65537	$2^{80}+1/65537$	64	15360	160	320

与 FNT 比较,变换长度有所增加. 表中同时给出了 Z_{M_2} 上的最大变换长度 N_{max}, 但相应的 α 可能不是简单的.

伪 FNT 是在整数环 $Z_{M_2}\left(M_2=\frac{M}{p_s^{l_s}},\ M=2^b+1\right)$ 上定义的数论变换,这种变换的模运算要比一般的 FNT 复杂些. 但是这个困难可以用下法避开. 如果注意到

$$M=p_1^{l_1}\cdot p_2^{l_2}\cdots p_s^{l_s},$$

那么下式是成立的:

$$X_{(\mathrm{mod}\,M/p_s^{l_s})}=\left(X_{(\mathrm{mod}\,M)}\right)_{(\mathrm{mod}\,M/p_s^{l_s})}. \tag{7}$$

这是因为,如果 $X=NM+X_{(\mathrm{mod}\,M)}$, 那么显然有

$$X-X_{(\mathrm{mod}\,M)}\equiv 0\left(\mathrm{mod}\,\frac{M}{p_s^{l_s}}\right).$$

由于(7)式成立, 故用伪 FNT 计算卷积时, 先按模 $M=2^b+1$ 进行计算, 得出的结果再对模 $M_2=\frac{M}{p_s^{l_s}}$ 进行模运算, 就可得到真值. 当按模 $M=2^b+1$ 进行计算时, 从表 5 可知, b 比有效字长 $\log_2 M_2$ 大 10%～20%.

当 b 为偶数时, $j=\sqrt{-1}\equiv 2^{\frac{b}{2}}\left(\mathrm{mod}\,\frac{M}{p_s^{l_s}}\right)$, 故亦可用伪 FNT 以 10 中的方法计算复数卷积.

—12—

复数数论变换(CNT)

利用实数数论变换，例如 FNT，可以计算两个复序列的卷积(参看**10**). 由于在许多应用中，例如雷达，声纳，通讯和遥感等，不能忽视信号的相位分量，计算复序列的变换就显得特别重要. 实数数论变换计算复序列的变换，是将实部与虚部分开分别计算. 本节研究复数数论变换，以便直接作复序列的变换.

一、复整数环 Z_M^C 的概念

设 M 为一自然数，以 M 为模的整数环 Z_M 定义为

$$Z_M=\{0,\ 1,\ 2,\ \cdots,\ M-1\}.$$

任一整数 a 必与且只与 Z_M 中一个整数模 M 同余，这个整数记作 $((a))$. 如果 $-\frac{M}{2}<a<\frac{M}{2}$，则

$$((a))=a.$$

设 $\quad Z_M^C=\{a+jb,\ a,\ b\in Z_M\},\quad j=\sqrt{-1}.$

任一复整数 Z (Z 的实部与虚部均为整数，则称 Z 为复整数，或称为 Gaussian 整数)必与且只与 Z_M^C 中的一个数相对应，记作 $[[Z]]$，即

$$[[Z]]=((\mathrm{Re}Z))+j((\mathrm{Im}Z)).$$

显然，如果

$$-\frac{M}{2}<\mathrm{Re}Z<\frac{M}{2},\quad -\frac{M}{2}<\mathrm{Im}Z<\frac{M}{2},$$

则 $$[[Z]]=Z.$$

同时，由定义得

$$[[Z_1+Z_2]]=[[Z_1]]+[[Z_2]],$$

$$[[Z_1\cdot Z_2]]=[[Z_1]]\cdot[[Z_2]].$$

其中 Z_1 和 Z_2 为任意两个复整数.

因此，称 Z_M^C 为复整数环.

二、复数数论变换

设 M 为任一自然数，$x_n\in Z_M^C$ $(n=0, 1, \cdots, N-1)$，称

$$X_k=\left[\left[\sum_{n=0}^{N-1}x_n\alpha^{nk}\right]\right] \quad (k=0, 1, \cdots, N-1), \qquad (1)$$

$$x_n=\left[\left[N^{-1}\sum_{k=0}^{N-1}X_k\alpha^{\langle -nk\rangle}\right]\right] \quad (n=0, 1, \cdots, N-1) \qquad (2)$$

为复数数论变换. 其中，$\alpha\in Z_M^C$，$\langle\cdot\rangle$ 表示模 N 的非负最小剩余.

不妨设 $N\geqslant 2$.

定理 1 设 M 为一自然数，当

1° N^{-1} 在 Z_M 上存在，即 $(N, M)=1$;

2° α 满足

$$[[\alpha]]^N=1, \qquad (3)$$

且 N 是使(3)式成立的最小正整数;

3° 存在 $\beta_t\in Z_M^C(t=1, 2, \cdots, N-1)$，使

$$[[\beta_t(\alpha^t-1)]]=1 \quad (t=1, 2, \cdots, N-1) \qquad (4)$$

时，(1)与(2)为一对互逆变换.

证明 将(2)式代入(1)式，有

$$X_k=\left[\left[\sum_{m=0}^{N-1}X_m\left(N^{-1}\sum_{n=0}^{N-1}\alpha^{nk+\langle -nm\rangle}\right)\right]\right]$$

$$=\left[\left[\sum_{m=0}^{N-1}X_m\left(N^{-1}\sum_{n=0}^{N-1}\alpha^{n\langle k-m\rangle}\right)\right]\right].$$

为要证明(1)与(2)是互逆变换，只需证明

$$\left[\left[N^{-1}\sum_{n=0}^{N-1}\alpha^{n\langle k-m\rangle}\right]\right]=\begin{cases}1, & k-m\equiv 0\ (\mathrm{mod}N),\\ 0, & k-m\not\equiv 0\ (\mathrm{mod}N).\end{cases}$$

由于条件 1° 与 2° 成立，故第一式显然成立. 为此只需证明

$$\left[\left[\sum_{n=1}^{N-1}\alpha^{n\langle t\rangle}\right]\right]=0.$$

事实上，只需证明

$$\left[\left[\sum_{n=0}^{N-1}\alpha^{nt}\right]\right]=0\quad (t=1,\ 2,\ \cdots,\ N-1).\tag{5}$$

由于有条件 3°，故

$$\left[\left[\sum_{n=0}^{N-1}\alpha^{nt}\right]\right]=[[\beta_t(\alpha^t-1)]]\left[\left[\sum_{n=0}^{N-1}\alpha^{nt}\right]\right]$$

$$=\left[\left[\beta_t(\alpha^t-1)\sum_{n=0}^{N-1}\alpha^{nt}\right]\right]$$

$$=[[\beta_t(\alpha^{Nt}-1)]]=[[\beta_t]][[\alpha^{tN}-1]]$$

$$=0\quad (t=1,\ 2,\ \cdots,\ N-1).$$

定理证毕*.

三、复数数论变换的循环卷积特性

设 $x_n\in Z_M^C$, $h_n\in Z_M^C(n=0,\ 1,\ \cdots,\ N-1)$. 称

$$y_n=\sum_{m=0}^{N-1}x_m h_{\langle n-m\rangle_N}\quad (n=0,\ 1,\ \cdots,\ N-1)\tag{6}$$

---

* 在定理的证明中，似乎只用到 $[[\alpha]]^N=1$，而并未用到"N 是使(3)式成立的最小自然数". 但这是必要的，如果对某个 $t(1\leqslant t\leqslant N-1)$，有 $[[\alpha]]^t=1$，那么由(5)式，将得到 $((N))=0$，但这与 $(N,\ M)=1$ 矛盾.

为复序列 $\{x_n\}$ 和 $\{h_n\}$ 的复数循环卷积.

定理 2 设

$$X_k=\left[\left[\sum_{n=0}^{N-1}x_n\alpha^{nk}\right]\right]$$

$$H_k=\left[\left[\sum_{n=0}^{N-1}h_n\alpha^{nk}\right]\right]\quad(k=0,\ 1,\ \cdots,\ N-1),$$

$$Y_k=\left[\left[\sum_{n=0}^{N-1}y_n\alpha^{nk}\right]\right]$$

则

$$Y_k=[[X_k\cdot H_k]]\quad(k=0,\ 1,\ \cdots,\ N-1).\tag{7}$$

证明

$$Y_k=\left[\left[\sum_{n=0}^{N-1}y_n\alpha^{nk}\right]\right]=\left[\left[\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}x_mh_{\langle n-m\rangle_N}\alpha^{nk}\right]\right].$$

记 $n-m=l$, 则

$$Y_k=\left[\left[\sum_{m=0}^{N-1}\sum_{l=-m}^{N-m-1}x_mh_{\langle l\rangle_N}\alpha^{(m+l)k}\right]\right].$$

由于
$$\left[\left[\sum_{l=-m}^{N-m-1}h_{\langle l\rangle_N}\alpha^{(m+l)k}\right]\right]=\left[\left[\sum_{l=0}^{N-1}h_l\alpha^{(m+l)k}\right]\right],$$

故
$$\begin{aligned}Y_k&=\left[\left[\sum_{m=0}^{N-1}\sum_{l=0}^{N-1}x_mh_l\alpha^{(m+l)k}\right]\right]\\&=\left[\left[\sum_{m=0}^{N-1}x_m\alpha^{mk}\right]\right]\cdot\left[\left[\sum_{l=0}^{N-1}h_l\alpha^{lk}\right]\right]\\&=[[X_k\cdot H_k]].\end{aligned}$$

证毕.

为了得到卷积的真值, 必须这样选取模 M, 即 M 必须满足

$$-\frac{M}{2}<\mathrm{Re}\left(\sum_{k=0}^{N-1}x_kh_{\langle n-k\rangle_N}\right),\quad \mathrm{Im}\left(\sum_{k=0}^{N-1}x_kh_{\langle n-k\rangle_N}\right)<\frac{M}{2}$$
$$(n=0,\ 1,\ \cdots,\ N-1).$$

如果记 $\tau=\max\limits_{0\leqslant n<N}|x_n|$, $\delta=\max\limits_{0\leqslant n<N}|h_n|$, 则 M 只需满足

$$-\frac{M}{2}<\tau\delta N<\frac{M}{2},$$

即

$$M > 2\tau\delta N. \tag{8}$$

四、复数 Mersenne 数变换

取 Mersenne 数为模，$M=M_p=2^p-1$，p 为素数，可以证明，N，α 可取如下值：

表 6

α	N	N^{-1}
2	p	$M_p-\frac{M_p-1}{p}$
-2	$2p$	$M_p-\frac{M_p-1}{2p}$
$2j$	$4p$	$M_p-\frac{M_p-1}{4p}$
$1+j$	$8p$	$M_p-\frac{M_p-1}{8p}$

下面分别加以证明．在 **8** 中，对前两种情况虽已经证明，但这里利用本节定理 1 来证明．

1．$\alpha=2$，$N=p$.

显然
$$((NN^{-1}))=((pM_p-M_p+1))$$
$$=(((p-1)2^p-p+2))=1.$$

由于 $[[\alpha^N]]=((2^p))=1$，p 为素数，显然 p 是这式成立的最小自然数．同时还可证明

$$(2^t-1,\ M_p)=1 \quad (t=1,\ 2,\ \cdots,\ p-1).$$

否则设对某个 $t(1\leqslant t\leqslant p-1)$，有

$$(2^t-1,\ M_p)=qd>1 \quad (q\text{ 为素数}),$$

于是有　　$2^t \equiv 1 \pmod q$,　　$2^p \equiv 1 \pmod q$,

由于 p 是素数,故 2 对模 q 的阶为 p, 从而有 $p|t$, 故 $t \geqslant p$, 但这与 t 的范围矛盾,因此

$$(2^t-1,\ M_p)=1 \quad (t=1,\ 2,\ \cdots,\ p-1).$$

这样,存在 $\beta_t \in Z_{M_p}$, 使

$$\beta_t(2^t-1) \equiv 1 (\bmod M_p) \quad (t=1,\ 2,\ \cdots,\ p-1),$$

即　　$$((\beta_t(2^t-1)))=1 \quad (t=1,\ 2,\ \cdots,\ p-1).$$

这样就证明了 $\{2,\ p\}$ 满足定理 1 的条件, 下列变换成立:

设 $x_n \in Z^C_{M_p}$ $(n=0,\ 1,\ \cdots,\ p-1)$, $M_p=2^p-1$, p 为素数,则

$$X_k=\left(\left(\sum_{n=1}^{N-1} a_n 2^{nk}\right)\right)+j\left(\left(\sum_{n=0}^{N-1} b_n 2^{nk}\right)\right)$$
$$(k=0,\ 1,\ \cdots,\ N-1), \tag{9}$$

$$x_n=\left(\left(N^{-1}\sum_{k=0}^{N-1} A_k 2^{\langle -nk\rangle}\right)\right)+j\left(\left(N^{-1}\sum_{k=0}^{N-1} B_k 2^{\langle -nk\rangle}\right)\right)$$
$$(n=0,\ 1,\ \cdots,\ N-1), \tag{10}$$

其中, $a_n=\mathrm{Re}(x_n)$, $b_n=\mathrm{Im}(x_n)$, $A_k=\mathrm{Re}(X_k)$, $B_k=\mathrm{Im}(X_k)$, $N=p$, $N^{-1}=M_p-\dfrac{M_p-1}{p}$.

2. $\alpha=-2$, $N=2p$.

显然　　$$((NN^{-1}))=1.$$

由于　　$$[[\alpha]]^{2p}=((-2))^{2p}=1,$$
$$[[\alpha]]^{p}=((-2))^{p}=-1,$$

所以 $\alpha=-2$ 对模 M_p 的阶数是 $N=2p$. 为了证明 $\alpha=-2$ 具有(4)所表示的性质,记

$$\lambda_t=((-2)^t-1) \quad (t=1,\ 2,\ \cdots,\ N-1),$$

只需证明

$$(\lambda_t, M_p)=1 \quad (t=1, 2, \cdots, N-1).$$

为此,

$$\lambda_t=\begin{cases}(\text{i})\ 2^{2n}-1, & t=2n, \quad 0<n<p,\\ (\text{ii})\ -(2^{2n+1}+1), & t=2n+1, \quad 0\leqslant n<p.\end{cases}$$

在(i)时,可以证明

$$(2^{2n}-1, M_p)=1 \quad (0<n<p).$$

否则,如对某个 $n(0<n<p)$, 有

$$(2^{2n}-1, M_p)=qd>1 \quad (q \text{ 是素数}),$$

于是有

$$2^{2n}\equiv 1 \pmod{q}, \quad 2^p\equiv 1 \pmod{q}.$$

由于 p 是素数, 2 对模 q 的阶数是 p, 从而有 $p|2n$, 即 $p|n$, 这表示 $n\geqslant p$, 这与 n 的范围矛盾.

故 $$(2^{2n}-1, M_p)=1 \quad (0<n<p).$$

在(ii)时,只需证明

$$(2^{2n+1}+1, M_p)=1 \quad (0\leqslant n<p).$$

事实上,可以证明

$$(1+2^k, M_p)=1 \quad (k \text{ 为任意自然数}),$$

为此,只需证明*

$$(1+2^k, M_p)=1 \quad (k=1, 2, \cdots, p-1).$$

同样可用反证法,如对 $0<k<p$ 中某个 k, 有

$$(1+2^k, M_p)=qd>1 \quad (q \text{ 是素数}),$$

和(i)的证法完全一样,得到 $k\geqslant p$, 这与 k 的范围矛盾. 故

$$(1+2^k, M_p)=1 \quad (k \text{ 为任意自然数}).$$

从而有 $$(1+2^{2n+1}, M_p)=1 \quad (0\leqslant n<p).$$

这样,由上证明,知

---

* 请参阅 117 页中的引理 1.

$$(\lambda_t,\ M_p)=1\quad(t=1,\ 2,\ \cdots,\ N-1).$$

记 β_t 为 λ_t 在 Z_{M_p} 上的逆元，于是

$$[[\beta_t\lambda_t]]=((\beta_t((-2)^t-1)))=1$$

$$(t=1,\ 2,\ \cdots,\ N-1).$$

所以，$\{-2,\ 2p\}$ 满足定理1的条件，如下变换成立：

设 $x_n\in Z_M^C\ (n=0,\ 1,\ \cdots,\ N-1)$，$M=M_p=2^p-1$，$p$ 是素数．则

$$X_k=\left[\left[\sum_{n=0}^{N-1}x_n(-2)^{nk}\right]\right]\quad(k=0,\ 1,\ \cdots,\ N-1),\qquad(11)$$

$$x_n=\left[\left[N^{-1}\sum_{k=1}^{N-1}X_k(-2)^{\langle -nk\rangle}\right]\right]$$

$$(n=0,\ 1,\ \cdots,\ N-1),\qquad(12)$$

其中，$N=2p$，$N^{-1}=M_p-\dfrac{M_p-1}{2p}$.

3．$\alpha=2j$，$N=4p$.

显然 $N=4p$ 是使 $[[\alpha]]^N=[[2j]]^{4p}=1$ 成立的最小正整数．只需证明 $\{\alpha=2j,\ N=4p\}$ 满足(4)．为了证明这点，先叙述如下三个引理，这些引理是容易证明的．

引理1 如果 $a\equiv b\ (\mathrm{mod}M)$，那么当 $(b,\ M)=1$ 时，有 $(a,\ M)=1$.

引理2 如果 $a|b$，那么当 $(b,\ M)=1$ 时，有 $(a,\ M)=1$.

引理3 当且仅当 $(a^2,\ M)=1$ 时，有 $(a,\ M)=1$.

上述三个引理中，a，b 均是整数，M 是自然数．

现在来证明 $\alpha=2j$，$N=4p$，具有(4)式表示的性质．记

$$\lambda_t=[1-(2j)^t][1-(-2j)^t]\quad(t=1,\ 2,\ \cdots,\ N-1).$$

如果能证明

$$(\lambda_t,\ M_p)=1\quad(t=1,\ 2,\ \cdots,\ N-1),\qquad(\mathrm{A1})$$

那么 λ_t 在 Z_{M_p} 中存在 λ_t^{-1}．记

$$\beta_t=\lambda_t^{-1}[(-2j)^t-1] \quad (t=1,\ 2,\ \cdots,\ N-1),$$

就有

$$[[\beta_t(\alpha^t-1)]]=[[\lambda_t^{-1}[(-2j)^t-1][(2j)^t-1]]]$$
$$=((\lambda_t^{-1}\lambda_t))=1 \quad (t=1,\ 2,\ \cdots,\ N-1).$$

因此，只需证明(A1)式.

为此，

$$\lambda_t=\begin{cases}(\text{i}) & (1-2^{4n})^2, & t=4n, & 0<n<p,\\ (\text{ii}) & 1+2^{8n+2}, & t=4n+1 & \\ (\text{iii}) & (1+2^{4n+2})^2, & t=4n+2 & 0\leqslant n<p;\\ (\text{iv}) & 1+2^{8n+6}, & t=4n+3 & \end{cases}$$

由于成立恒等式：

$$(2^{2s+1}+2^{s+1}+1)(2^{2s+1}-2^{s+1}+1)=2^{4s+2}+1, \qquad (\text{A2})$$

因此，λ_t 可整除 σ_t:

$$\sigma_t=\begin{cases}(\text{i}) & (1-2^{4n})^2, & t=4n, & 0<n<p,\\ (\text{ii}) & 1+2^{8n+2}, & t=4n+1 & \\ (\text{iii}) & 1+2^{16n+10}, & t=4n+2 & 0\leqslant n<p.\\ (\text{iv}) & 1+2^{8n+6}, & t=4n+3 & \end{cases}$$

根据引理 2，如果能证明

$$(\sigma_t,\ M_p)=1 \quad (t=1,\ 2,\ \cdots,\ N-1),$$

那么(A1)成立.

除去(i)以外，σ_t 具有形状

$$2^k+1.$$

由于在上段中已经证明

$$(2^k+1,\ M_p)=1 \quad (k\ \text{为任意数}), \qquad (\text{A3})$$

因此在(ii)→(iv)，均有

$$(\sigma_t,\ M_p)=1.$$

直接证明(i). 根据引理 3，只需证明

$$(1-2^{4n},\ M_p)=1 \quad (0<n<p). \tag{A4}$$

如果不是这样，设对某个 $n(0<n<p)$，有

$$(1-2^{4n},\ M_p)=qd>1 \quad (q\text{ 是素数}).$$

于是有 $\qquad 2^{4n}\equiv 1 \pmod{q}, \quad 2^p\equiv 1 \pmod{q}.$

由于 2 对模 q 的阶是 p，故 $p|4n$，即 $p|n$，从而 $n\geqslant p$. 但这与 n 的范围矛盾. 故(A4)式成立，从而

$$((1-2^{4n})^2,\ M_p)=1 \quad (0<n<p).$$

这样就证明了

$$(\sigma_t,\ M_p)=1 \quad (t=1,\ 2,\ \cdots,\ N-1),$$

从而 $\qquad (\lambda_t,\ M_p)=1 \quad (t=1,\ 2,\ \cdots,\ N-1).$

因而 $\{\alpha=2j,\ N=4p\}$ 具有(4)式的性质. 故如下变换成立：

设 $x_n\in Z^c_{M_p}(n=0,\ 1,\ 2,\ \cdots,\ N-1)$，有

$$X_k=\left[\left[\sum_{n=0}^{N-1}x_n\alpha^{nk}\right]\right] \quad (k=0,\ 1,\ \cdots,\ N-1), \tag{13}$$

$$x_n=\left[\left[N^{-1}\sum_{k=0}^{N-1}X_n\alpha^{\langle -nk\rangle}\right]\right] \quad (n=0,1,\cdots,N-1), \tag{14}$$

其中，$\alpha=2j,\ N=4p,\ N^{-1}=M_p-\dfrac{M_p-1}{4p}$.

4. $\alpha=1+j,\ N=8p$.

只需证明 $\{\alpha=1+j,\ N=8p\}$ 具有 (4) 式所表示的性质. 为此，记

$$\lambda_t=[(1+j)^t-1][(1-j)^t-1] \quad (t=0,\ 1,\ \cdots,\ N-1),$$

λ_t 是实数. 如果能证明

$$(\lambda_t,\ M_p)=1 \quad (t=1,\ 2,\ \cdots,\ N-1), \tag{A5}$$

那么在 Z_{M_p} 中，存在 λ_t^{-1}，令

$$\beta_t=\lambda_t^{-1}[(1-j)^t-1] \quad (t=1,\ 2,\ \cdots,\ N-1),$$

就有

$$
\begin{aligned}
&[[\beta_t[(1+j)^t-1]]] \\
&\quad=[[\lambda_t^{-1}[(1-j)^t-1][(1+j)^t-1]]] \\
&\quad=((\lambda_t^{-1}\lambda_t))=1 \quad (t=1,\ 2,\ \cdots,\ N-1).
\end{aligned}
$$

这就表明 $\{\alpha=1+j,\ N=8p\}$ 具有(4)式的性质.

由于有

$$
\lambda_t=\begin{cases}
(\text{i})\ (1-2^{4n})^2, & t=8n, \quad 0<n<p, \\
(\text{ii})\ 1-2^{4n+1}+2^{8n+1}, & t=8n+1 \\
(\text{iii})\ 1+2^{8n+2}, & t=8n+2 \\
(\text{iv})\ 1+2^{4n+2}+2^{8n+3}, & t=8n+3 \\
(\text{v})\ (1+2^{4n+2})^2, & t=8n+4 \quad \Big\}\ 0\leqslant n<p; \\
(\text{vi})\ 1+2^{4n+3}+2^{8n+5}, & t=8n+5 \\
(\text{vii})\ 1+2^{8n+6}, & t=8n+6 \\
(\text{viii})\ 1-2^{4n+4}+2^{8n+7}, & t=8n+7
\end{cases}
\tag{A6}
$$

又由于恒等式(A2), λ_t 能整除 σ_t:

$$
\sigma_t=\begin{cases}
(\text{i})\ (1-2^{4n})^2, & t=8n, \quad 0<n<p, \\
(\text{ii})\ 1+2^{16n+2}, & t=8n+1 \\
(\text{iii})\ 1+2^{8n+2}, & t=8n+2 \\
(\text{iv})\ 1+2^{16n+6}, & t=8n+3 \\
(\text{v})\ (1+2^{4n+2})^2, & t=8n+4 \quad \Big\}\ 0\leqslant n<p. \\
(\text{vi})\ 1+2^{16n+10}, & t=8n+5 \\
(\text{vii})\ 1+2^{8n+6}, & t=8n+6 \\
(\text{viii})\ 1+2^{16n+14}, & t=8n+7
\end{cases}
\tag{A7}
$$

根据引理 2 及(A3)式, 知除去(i)与(v)外, 有

$$(\lambda_t,\ M_p)=1.$$

又根据引理 3 及(A3), (A4), 知(i)和(v)也成立:

$$(\lambda_t,\ M_p)=1.$$

因此，有

$$(\lambda_t,\ M_p)=1 \quad (t=1,\ 2,\ \cdots,\ N-1).$$

这就是所要证明的. 于是如下变换成立：

设 $x_n \in Z^C_{M_p}(n=0,\ 1,\ \cdots,\ N-1)$，则

$$X_k=\left[\left[\sum_{n=0}^{N-1} x_n \alpha^{nk}\right]\right] \quad (k=0,\ 1,\ \cdots,\ N-1), \tag{15}$$

$$x_n=\left[\left[N^{-1}\sum_{k=0}^{N-1} X_k \alpha^{\langle -nk\rangle}\right]\right] \quad (n=0,\ 1,\ \cdots,\ N-1), \tag{16}$$

其中，$\alpha=1+j$，$N=8p$，$N^{-1}=M_p-\dfrac{M_p-1}{8p}$.

五、复数 Fermat 数变换

取 Fermat 数为模，$M=F_k=2^b+1$，$b=2^k$，k 为自然数. 可以证明 α、N 可取如下值：

表 7

α	N	N^{-1}
2	$2b=2^{k+1}$	$2^{2^{k+1}-(k+1)}$
$\sqrt{2}$	$4b=2^{k+2}$	$2^{2^{k+2}-(k+2)}$
$1+j$	$4b=2^{k+2}$	$2^{2^{k+2}-(k+2)}$
3	2^{2^k}	2^{2^k}*

其中，$\sqrt{2}=2^{\frac{b}{4}}(2^{\frac{b}{2}}-1)$，$k\geqslant 2$.

1. $\alpha=2$，$N=2b=2^{k+1}$.

由于 $((2))^N=((2^{2b}))=((2^{2^{k+1}}))=(-1)^2=1$,

* 这是当 $1\leqslant k\leqslant 4$ 时的情况.

$$((2))^{\frac{N}{2}}=((2^b))=-1,$$

故 2 对模 F_k 的阶是 $2b$. 同时,还可证明

$$(\alpha^t-1,\ F_k)=(2^t-1,\ F_k)=1$$
$$(t=1,\ 2,\ \cdots,\ N-1).$$

因为如果存在一个 $t(1\leqslant t\leqslant N-1)$, 使

$$(2^t-1,\ F_k)=qd>1,$$

其中 q 不妨设为 F_k 的一个素因子. 于是有

$$2^t\equiv 1\quad(\mathrm{mod}\,q),$$

$$2^{2^k}\equiv -1\quad(\mathrm{mod}\,q)\quad 即\quad 2^{2^{k+1}}\equiv 1\quad(\mathrm{mod}\,q).$$

可以证明, 2 对模 q 的阶是 2^{k+1} (参阅 **9**). 因此 $2^{k+1}|t$, 这表示 $t\geqslant 2^{k+1}=2b$, 与 t 的范围矛盾. 因此 $(2^t-1,\ F_k)=1$ $(t=1,\ 2,\ \cdots,\ N-1)$. 这表示 2^t-1 在 Z_M 中存在逆元,记为 β_t, 有

$$((\beta_t(2^t-1)))=1\quad(t=1,\ 2,\ \cdots,\ N-1).$$

这表示 $\{\alpha=2,\ N=2b\}$ 满足定理 1 的条件, 因此如下变换成立:

设 $x_n\in Z_M^C(n=0,\ 1,\ \cdots,\ N-1)$, $M=F_k=2^b+1$, $b=2^k$, k 为自然数, 则

$$X_k=\left[\left[\sum_{n=0}^{N-1}x_n2^{nk}\right]\right]\quad(k=0,\ 1,\ \cdots,\ N-1),\tag{17}$$

$$x_n=\left[\left[N^{-1}\sum_{k=0}^{N-1}X_k2^{\langle -nk\rangle}\right]\right]\quad(n=0,\ 1,\ \cdots,\ N-1),\tag{18}$$

其中, $N=2b$, $N^{-1}=2^{2^{k+1}-(k+1)}$.

2. $\alpha=\sqrt{2}$, $N=4b=2^{k+2}$, $k>1$.

这里 $\alpha=\sqrt{2}=2^{\frac{b}{4}}(2^{\frac{b}{2}}-1)$ 为一整数, 由于

$$[[\alpha]]^N=((\sqrt{2}))^{4b}=1,$$

$$[[\alpha]]^{\frac{N}{2}}=((\sqrt{2}))^{2b}=-1,$$

所以 $\alpha=\sqrt{2}$ 对模 F_k 的阶为 $4b$. 下面证明

$$\{\alpha=\sqrt{2},\quad N=4b\}$$

满足(4)所表示的性质.

记

$$\lambda_t=((\sqrt{2})^t-1)\quad(t=1,\ 2,\ \cdots,\ N-1),$$

只需证明 $\quad(\lambda_t,\ F_k)=1\quad(t=1,\ 2,\ \cdots,\ N-1)$.

因为

$$\lambda_t=\begin{cases}(\text{i})\ 2^n-1, & t=2n,\quad 0<n<2^{k+1},\\ (\text{ii})\ 2^{n+\frac{1}{2}}-1, & t=2n+1,\quad 0\leqslant n<2^{k+1},\end{cases}$$

在(i)时, 上段已证明有

$$(2^n-1,\ F_k)=1\quad(n=1,\ 2,\ \cdots,\ 2^{k+1}-1),$$

在(ii)时, 如果有一个 $n\ (0\leqslant n<2^{k+1})$, 使

$(2^{n+\frac{1}{2}}-1,\quad F_k)=qd>1$ (q 不妨设为 F_k 的素因子),

于是有 $2^{n+\frac{1}{2}}\equiv1(\text{mod}q)$, 即 $2^{2n+1}\equiv1(\text{mod}q)$, 由于 2^{k+1} 是 2 对模 q 的阶, 便有

$$2^{k+1}|2n+1,$$

但这不可能成立. 因此 $(2^{n+\frac{1}{2}}-1,\ F_k)=1\ (n=0,\ 1,\ \cdots,\ 2^{k+1}-1)$. 这样便证明了

$$(\lambda_t,\ F_k)=1\quad(t=1,\ 2,\ \cdots,\ N-1).$$

所以, $\{\alpha=\sqrt{2},\ N=4b\}$ 满足定理 1 的条件.

3. $\alpha=1+j$, $N=4b=2^{k+2}$, k 为自然数.

显然 $N=4b$ 是使

$$[[\alpha]]^N=[[1+j]]^{4b}=1$$

成立的最小自然数. 下面证明 $\{\alpha=1+j,\ N=4b\}$ 满足(4)所表示的性质.

设

$$\lambda_t=[(1+j)^t-1][(1-j)^t-1] \quad (t=1,\ 2,\ \cdots,\ N-1),$$

λ_t 是一个实数. 如果能证明

$$(\lambda_t,\ F_k)=1 \quad (t=1,\ 2,\ \cdots,\ N-1),$$

那么 λ_t 在 Z_{F_k} 中存在逆元 λ_t^{-1}. 记

$$\beta_t=\lambda_t^{-1}[(1-j)^t-1] \quad (t=1,\ 2,\ \cdots,\ N-1),$$

于是就有

$$\begin{aligned}&[[\beta_t[(1+j)^t-1]]]\\ &\quad=[[\lambda_t^{-1}[(1-j)^t-1][(1+j)^t-1]]]\\ &\quad=((\lambda_t^{-1}\lambda_t))=1.\end{aligned}$$

λ_t 如(A6)所示. 利用恒等式(A2), λ_t 能整除 σ_t:

$$\sigma_t=\begin{cases}(\text{i})\ (1-2^{4n})^2, & t=8n \qquad 0<n<2^{k-1},\\ (\text{ii})\ 1+2^{16n+2}, & t=8n+1\\ (\text{iii})\ 1+2^{8n+2}, & t=8n+2\\ (\text{iv})\ 1+2^{16n+6}, & t=8n+3\\ (\text{v})\ (1+2^{4n+2})^2, & t=8n+4 \qquad 0\leqslant n<2^{k-1}.\\ (\text{vi})\ 1+2^{16n+10}, & t=8n+5\\ (\text{vii})\ 1+2^{8n+6}, & t=8n+6\\ (\text{viii})\ 1+2^{16n+14}, & t=8n+7\end{cases}$$

设 $M=F_k=2^b+1(b=2^k,\ k>1$ 自然数), 并设 q 是 F_k 的一个素因子, 那么 2 对模 q 的阶是 2^{k+1}. 在(ii)的情况下, 如对某个 $n(0\leqslant n<2^{k-1})$, 有

$$(2^{16n+2}+1,\ F_k)=qd>1,$$

那么就有

$$2^{16n+2}\equiv-1 \pmod{q}, \quad 即 2^{32n+4}\equiv1 \pmod{q}.$$

因此 $2^{k+1}|32n+4$, 这个式子只有当 $k\leqslant1$ 时才成立, 但这与 k 的范围矛盾. 这表示

$$(2^{16n+2}+1,\ F_k)=1, \quad 0\leqslant n<2^{k-1}.$$

同理可证(iii)→(viii).

在(i)的情况下,假设对 $0<n<2^{k-1}$ 中的某个 n 有

$$(1-2^{4n},\ F_k)=qd>1,$$

那么有

$$2^{4n}\equiv 1 \pmod{q}.$$

于是 $2^{k+1}|4n$, 即 $n\geqslant 2^{k-1}$. 但这同样与 n 的范围矛盾. 因此 $(1-2^{4n},\ F_k)=1,\ 0<n<2^{k-1}$. 根据引理 3, 知

$$((1-2^{4n})^2,\quad F_k)=1,\quad 0<n<2^{k-1}.$$

这样就证明了

$$(\lambda_t,\ F_k)=1 \quad (t=1,\ 2,\ \cdots,\ N-1).$$

故 $\{\alpha=1+j,\ N=4b\}$ 满足定理 1 的条件.

4. $\alpha=3,\ N=2^{2^k}(1\leqslant k\leqslant 4)$.

这在 **9** 中已经证明.

本节讨论的复数数论变换是在 **3** 中初等数论的基本知识的基础上进行的,而没有用到一般二次数域的知识,相信读者都能理解. 得到的结果(定理 1)还是比较简单的. 我们特别详细的证明了复数 Mersenne 数变换和复数 Fermat 数变换的各种情况. 从表 6 清楚的看到, 在模 M 相同的情况下(也就是字长相同的情况下), α 取复数值, 可计算的序列长度 N 成倍的增加. 如果还想增加 N, 还是可以办得到的, 不过 α 这时可能不是简单的,反而失去 NTT 的优点.

复数数论变换的主要应用是计算复序列的卷积, 关于这方面的具体例子,读者可参阅 **15**.

我们还可以应用 **11** 的思想来讨论复伪数论变换. 下面我们简单考虑一下复伪 FNT.

设 $M=2^b+1(b\neq 2^t,\ b$ 为奇整数), 考虑在模 $M_2=M/p_s^{l_s}$ 上定义的伪 FNT, 设其参数为

$$\left\{\alpha=2^w,\quad N=\frac{2b}{w}\right\},$$

其中 w 为奇数. 在这条件下，由于 $Nw=2b$，故 N 是偶数，$\frac{N}{2}$ 是奇数.

设 $Z_{M_2}^C$ 是以 M_2 为模的复整数环，在上述条件下，可以证明 $\{(1+j)^w,\ 4N\}=\left\{(1+j)^w,\ \frac{8b}{w}\right\}$ 满足复数数论变换的条件. 事实上，$4N$ 是使下式成立的最小正整数：

$$[[(1+j)^w]]^{4N}=1.$$

这是因为

$$\begin{aligned}
[[(1+j)^w]]^{4N}&=(((1+j)^{4wN}))=(((2j)^{2wN}))\\
&=(((-1)^{2b}2^{4b}))=((2^{4b}))=1,\\
[[(1+j)^w]]^{2N}&=(((1+j)^{2wN}))=(((2j)^{wN}))\\
&=(((-1)^b2^{2b}))=-((2^{2b}))=-1.
\end{aligned}$$

与前面一样，可证明 $\{(1+j)^w,\ 4N\}$ 满足(4)式所表示的性质. 又由假设 N 在 Z_{M_2} 中存在逆元，4 与 M 互素，故 $4N$ 在 Z_{M_2} 中存在逆元 $(4N)^{-1}$. 因此下述变换成立：设

$$x_n\in Z_{M_2}^C\quad(n=0,\ 1,\ \cdots,\ 4N-1),$$

$$X_k=\left[\left[\sum_{n=0}^{4N-1}(1+j)^{wnk}x_n\right]\right]\quad(k=0,\ 1,\ \cdots,\ 4N-1),$$

$$x_n=\left[\left[(4N)^{-1}\sum_{k=1}^{4N-1}(1+j)^{\langle -wnk\rangle}X_k\right]\right]$$

$$(n=0,\ 1,\ \cdots,\ 4N-1).$$

应用复伪 FNT，可作变换及卷积的长度比实的 FNT 或复 FNT 的长度要增加一倍. 具体地说，$w=1$ 时，实的 FNT 以 $\sqrt{2}=2^{\frac{b}{2}}(2^{\frac{b}{4}}-1)$ 为根以及复 FNT 以 $\alpha=1+j$ 为根时，最大长度是 $4b$，而复伪 FNT 以 $\alpha=1+j$ 为根时，最大长度是

表 8　当 b 是奇数时，在 $Z^C_{M_2}(M_2=2^b+1/p_s^{l_s})$ 上的复伪 FNT 的各种参数

b	$M=2^b+1$ 的分解式 $M=p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s}$	M_1	M_2	有效字长 $\log_2 M_2$ (约)	变换长度	复数根
15	$3^2\cdot11\cdot331$	3^2	$\frac{2^{15}+1}{3^2}$	12	40 $(2^3\cdot5)$	$2(j-1)$
21	$3^2\cdot43\cdot5419$	3^2	$\frac{2^{21}+1}{3^2}$	18	56 $(2^3\cdot7)$	$2(j-1)$
25	$3\cdot11\cdot251\cdot4051$	$3\cdot11$	$\frac{2^{25}+1}{3\cdot11}$	20	200 $(2^3\cdot5^2)$	$j+1$
27	$3^4\cdot19\cdot87211$	$3^4\cdot19$	$\frac{2^{27}+1}{3^4\cdot19}$	16	216 $(2^3\cdot3^3)$	$j+1$
29	$3\cdot59\cdot3033169$	3	$\frac{2^{29}+1}{3}$	27	232 $(2^3\cdot29)$	$j+1$
33	$3^2\cdot67\cdot683\cdot20857$	3^2	$\frac{2^{33}+1}{3^2}$	30	88 $(2^3\cdot11)$	$2(j-1)$
35	$3\cdot11\cdot43\cdot281\cdot86171$	$3\cdot11$	$\frac{2^{35}+1}{3\cdot11}$	30	56 $(2^3\cdot7)$	$-2^2(1+j)$
41	$3\cdot83\cdot8831418697$	3	$\frac{2^{41}+1}{3}$	39	328 $(2^3\cdot41)$	$j+1$
45	$3^3\cdot11\cdot19\cdot331\cdot18837001$	$3^3\cdot19$	$\frac{2^{45}+1}{3^3\cdot19}$	36	40 $(2^3\cdot5)$	$2^4(1+j)$
49	$3\cdot43\cdot4363953127297$	$3\cdot43$	$\frac{2^{49}+1}{3\cdot43}$	41	392 $(2^3\cdot7^2)$	$j+1$

$8b$. 同时，FNT 和复 FNT 的字长是 $b=2^t$，可供选择的字长太少，而复伪 FNT，字长 b 的选择却灵活得多(见表 8).

表 8 列出了部分复伪 FNT 的参数. 从表中可以看出，当 b 是素数且 $\alpha=1+j$ 时，变换长度是 $8b$，这些数并非高度复合数. 当 b 非素数时，相应的 N 既大且可高度分解因子，因而可用类似 DFT 的快速算法. 特别以 $(2^{25}+1)/3\cdot 11$ 和 $(2^{49}+1)/3\cdot 43$ 为模定义的 200 点和 392 点的变换最为实用.

—13—

二维及多维数论变换

前面我们详细的讨论了一维数论变换，其中特别对 Mersenne 数变换及 Fermat 数变换进行了研究，并且还讨论了复数数论变换．我们已经看到，在一维信号处理过程中，Fermat 数变换是特别有前途的． FNT 的模 $M=F_t=2^b+1$ $(b=2^t)$ 的字长 b 不够灵活这个缺点，我们利用伪 FNT 及复伪 FNT 进行了一些改善． 但是当用 FNT 来计算长序列的一维卷积时，所需的字长 b 与序列长度 N 成正比，当 N 较大时，b 也较大． 例如 $N=1024$ 时，b 至少为 256，这甚至是无法实现的． 然而，如果我们用二维数论变换来实现一维循环卷积，那么所需字长 b 将与序列长度 N 的平方根成正比，而如果用三维数论变换，则 b 将与 N 的立方根成正比，因此一维卷积多维处理可以大大减少所需的字长．另外当用数字电子计算机进行信号处理时，如果信号及噪声是二元函数（如图象处理），那么就需要计算二维卷积，二维卷积可以用二维变换法实现． 因此，我们有必要把一维数论变换推广到二维及多维的情形．

为了易于读者理解，我们从二维卷积的定义开始． 本节第一段中的引理 1 及引理 2 是将一般二维卷积及二维恒定对角卷积通过补零的办法化为二维循环卷积，二维循环卷积可以用变换法实现．第二段简要的叙述一下二维 DFT，第三段才是二维及多维数论变换．

一、二维卷积和二维循环卷积

设(x)和(h)分别是由$x(n, m)$和$h(n, m)$($n=0, 1, \cdots, N-1$; $m=0, 1, \cdots, M-1$)组成的$N\times M$数阵，且有

$$x(n, m)=h(n, m)=0 \quad (n<0 \text{或} m<0),$$

记

$$(x)=\{x(n, m)\}_{N\times M}=\begin{bmatrix} x(0, 0) & x(0, 1) & \cdots x(0, M-1) \\ x(1, 0) & x(1, 1) & \cdots x(1, M-1) \\ \vdots & \vdots & \vdots \quad \vdots \\ x(N-1, 0) & x(N-1, 1) & \cdots x(N-1, M-1) \end{bmatrix}, \tag{1}$$

$$(h)=\{h(n, m)\}_{N\times M}=\begin{bmatrix} h(0, 0) & h(0, 1) & \cdots h(0, M-1) \\ h(1, 0) & h(1, 1) & \cdots h(1, M-1) \\ \vdots & \vdots & \vdots \quad \vdots \\ h(N-1, 0) & h(N-1, 1) & \cdots h(N-1, M-1) \end{bmatrix}, \tag{2}$$

这两个数阵的二维卷积是指：

$$\begin{aligned} y(r, s) &= \sum_{n=0}^{N-1}\sum_{m=0}^{M-1} x(n, m)h(r-n, s-m) \\ &= \sum_{n=0}^{N-1}\sum_{m=0}^{M-1} x(r-n, s-m)h(n, m) \end{aligned} \tag{3}$$

$$\begin{pmatrix} r=0, 1, \cdots, N-1 \\ s=0, 1, \cdots, M-1 \end{pmatrix}.$$

二维卷积$y(r, s)$也是$N\times M$数阵，记为：

$$(y)=\{y(r,\ s)\}_{N\times M}$$

$$=\begin{bmatrix} y(0,\ 0) & y(0,\ 1) & \cdots & y(0,\ M-1) \\ y(1,\ 0) & y(1,\ 1) & \cdots & y(1,\ M-1) \\ \vdots & \vdots & \vdots & \vdots \\ y(N-1,\ 0) & y(N-1,\ 1) & \cdots & y(N-1,\ M-1) \end{bmatrix}. \quad (4)$$

式(3)可用矩阵形式表示，(y)的第 k 列元素是

$$\begin{bmatrix} y(0,\ k) \\ y(1,\ k) \\ y(2,\ k) \\ \vdots \\ y(N-1,\ k) \end{bmatrix}$$

$$=\sum_{m=0}^{k}\begin{bmatrix} h(0,\ k-m) & & & \\ h(1,\ k-m) & h(0,\ k-m) & & \text{\huge 0} \\ h(2,\ k-m) & h(1,\ k-m) & & \\ \vdots & \vdots & & \\ h(N-1,\ k-m) & h(N-2,\ k-m) & \cdots & h(0,\ k-m) \end{bmatrix}$$

$$\cdot\begin{bmatrix} x(0,\ m) \\ x(1,\ m) \\ x(2,\ m) \\ \vdots \\ x(N-1,\ m) \end{bmatrix} \quad (k=0,\ 1,\ \cdots,\ M-1). \quad (5)$$

这种二维卷积就是二维数字滤波所遇到的，通常可以用二维循环卷积来计算.

所谓两个数阵(x)和(h)的二维循环卷积是指:

$$y(r, s)=\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}x(n, m)h[\langle r-n\rangle_N, \langle s-m\rangle_M]$$

$$=\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}x[\langle r-n\rangle_N, \langle s-m\rangle_M]h(n, m)$$

$$\begin{pmatrix} r=0, 1, \cdots, N-1 \\ s=0, 1, \cdots, M-1 \end{pmatrix}. \tag{6}$$

引理1 设(x)和(h)为$N\times M$数阵

$$(x)=\{x(n, m)\}_{N\times M}, \quad (h)=\{h(n, m)\}_{N\times M},$$

它们的二维卷积(3)可以通过如下的两个$2N\times 2M$数阵$(\hat{x})$和$(\hat{h})$的二维循环卷积来计算.

设

$$\hat{x}(n, m)=\begin{cases} x(n, m)\begin{pmatrix} n=0, 1, \cdots, N-1 \\ m=0, 1, \cdots, M-1 \end{pmatrix}, \\ 0, \qquad\qquad \text{其它}; \end{cases} \tag{7}$$

$$\hat{h}(n, m)=\begin{cases} h(n, m)\begin{pmatrix} n=0, 1, \cdots, N-1 \\ m=0, 1, \cdots, M-1 \end{pmatrix}, \\ 0, \qquad\qquad \text{其它}. \end{cases} \tag{7'}$$

$(\hat{x})$和$(\hat{h})$的二维循环卷积为

$$\hat{y}(r, s)=\sum_{n=0}^{2N-1}\sum_{m=0}^{2M-1}\hat{x}(n, m)\hat{h}[\langle r-n\rangle_{2N}, \langle s-m\rangle_{2M}]$$

$$\begin{pmatrix} r=0, 1, \cdots, 2N-1 \\ s=0, 1, \cdots, 2M-1 \end{pmatrix}, \tag{8}$$

则

$$y(r, s)=\hat{y}(r, s)\begin{pmatrix} r=0, 1, \cdots, N-1 \\ s=0, 1, \cdots, M-1 \end{pmatrix}. \tag{9}$$

证明 由(7)式，当 $r=0, 1, \cdots, N-1; s=0,1,\cdots,M-1$ 时，有

$$\hat{y}(r, s)=\sum_{n=0}^{2N-1}\sum_{m=0}^{2M-1}\hat{x}(n, m)\hat{h}[\langle r-n\rangle_{2N}, \langle s-m\rangle_{2M}]$$

$$=\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}x(n, m)\hat{h}[\langle r-n\rangle_{2N}, \langle s-m\rangle_{2M}].$$

由于当 $r, n=0, 1, \cdots, N-1$; $s, m=0, 1, \cdots, M-1$ 时，有

$$-(N-1)\leqslant r-n\leqslant N-1,$$

$$-(M-1)\leqslant s-m\leqslant M-1,$$

由(7′)式，有

$$\hat{h}[\langle r-n\rangle_{2N}, \langle s-m\rangle_{2M}]$$

$$=\begin{cases} h(r-n, s-m)\begin{pmatrix}0\leqslant r-n\leqslant N-1\\ 0\leqslant s-m\leqslant M-1\end{pmatrix}, \\ 0, \qquad\qquad\qquad \text{其它}. \end{cases}$$

因此，

$$\hat{y}(r, s)=\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}x(n, m)h(r-n, s-m)$$

$$\begin{pmatrix}0\leqslant r-n\leqslant N-1\\ 0\leqslant s-m\leqslant M-1\end{pmatrix}.$$

注意到当 $n<0$ 或 $m<0$ 时，$h(n, m)=0$，于是

$$\hat{y}(r, s)=\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}x(n, m)h(r-n, s-m)=y(r, s).$$

证毕.

引理 1 中的数阵$(\hat{x})$和$(\hat{h})$是由(x)和(h)通过补零形成的. $(\hat{x})$和$(\hat{h})$分别是

$$(\hat{x})=\left[\overbrace{\begin{matrix} x(0,0) & x(0,1) & \cdots & x(0,M-1) & 0\cdots 0 \\ x(1,0) & x(1,1) & \cdots & x(1,M-1) & 0\cdots 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x(N-1,0) & x(N-1,1) & \cdots & x(N-1,M-1) & 0\cdots 0 \\ 0 & 0 & \cdots & 0 & 0\cdots 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots\quad\vdots \\ 0 & 0 & \cdots & 0 & 0\quad 0 \end{matrix}}^{2M}\right]\left.\vphantom{\begin{matrix}1\\1\\1\\1\\1\\1\\1\end{matrix}}\right\}2N,$$

$$(\hat{h})=\left[\overbrace{\begin{matrix} h(0,0) & \cdots & h(0,M-1) & 0\cdots 0 \\ \vdots & \vdots & \vdots & \vdots\quad\vdots \\ h(N-1,0) & \cdots & h(N-1,M-1) & 0\cdots 0 \\ 0 & \cdots & 0 & 0\cdots 0 \\ \vdots & \vdots & \vdots & \vdots\quad\vdots \\ 0 & \cdots & 0 & 0\cdots 0 \end{matrix}}^{2M}\right]\left.\vphantom{\begin{matrix}1\\1\\1\\1\\1\\1\end{matrix}}\right\}2N.$$

$(\hat{x})$和$(\hat{h})$的循环卷积$(\hat{y})$的左上角$N\times M$子数阵在数值上就是(x)和(h)的卷积(y)的值.

在实际应用中，还可能遇到一种有别于二维卷积 (3) 和二维循环卷积 (6) 的一种卷积，这种卷积称为二维恒定对角卷积:

$$y(r,s)=\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}x(n,m)h(r-n,s-m)$$
$$\left(\begin{matrix} r=0,1,\cdots,N-1 \\ s=0,1,\cdots,M-1 \end{matrix}\right). \tag{10}$$

(10)式中下标出现负值时，不再如(3)式那样h值为零，也不再如(6)式那样h值是周期的. 二维卷积(3)和二维循环卷积(6)都是这种卷积的特殊情况. 式(10)是如下$N\times M$数阵(x)和$(2N-1)\times(2M-1)$数阵(h)之间的一种运算:

$$
(x)=\{x(n,\ m)\}_{N\times M}
=\begin{bmatrix}
x(0,\ 0) & x(0,\ 1) & \cdots & x(0,\ M-1)\\
x(1,\ 0) & x(1,\ 1) & \cdots & x(1,\ M-1)\\
\vdots & \vdots & \vdots & \vdots\\
x(N-1,\ 0) & x(N-1,\ 1) & \cdots & x(N-1,\ M-1)
\end{bmatrix}, \tag{11}
$$

$$
(h)=\{h(n,\ m)\}_{(2N-1)\times(2M-1)}
=\left.\begin{bmatrix}
\overbrace{h(-N+1,-M+1) & h(-N+1,-M+2) & \cdots & h(-N+1,0) & \cdots & h(-N+1,M-1)}^{2M-1}\\
h(-N+2,-M+1) & h(-N+2,-M+2) & \cdots & h(-N+2,0) & \cdots & h(-N+2,M-1)\\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\
h(0,\ -M+1) & h(0,\ -M+2) & \cdots & h(0,\ 0) & \cdots & h(0,\ M-1)\\
h(1,\ -M+1) & h(1,\ -M+2) & \cdots & h(1,\ 0) & \cdots & h(1,\ M-1)\\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\
h(N-1,\ -M+1) & h(N-1,\ -M+2) & \cdots & h(N-1,\ 0) & \cdots & h(N-1,\ M-1)
\end{bmatrix}\right\}2N-1 \tag{12}
$$

引理 2 设数阵(x)和(h)如(11)式和(12)式所示，其恒定对角卷积(10)式可通过如下定义的两个$2N\times 2M$数阵$(\hat{x})$和$(\hat{h})$的循环卷积来计算.

设

$$\hat{x}(n, m)=\begin{cases} x(n, m)\begin{pmatrix} n=0, 1, \cdots, N-1 \\ m=0, 1, \cdots, M-1 \end{pmatrix}, \\ 0, \qquad\qquad \text{其它}; \end{cases} \tag{13}$$

$$\hat{h}(n, m)=\begin{cases} 0, \quad n=0 \quad \text{或} \quad m=0, \\ h(-N+n, -M+m)\begin{pmatrix} n=1, 2, \cdots, 2N-1 \\ m=1, 2, \cdots, 2M-1 \end{pmatrix}. \end{cases} \tag{14}$$

$(\hat{x})$和$(\hat{h})$的循环卷积记为$(\hat{y})$，即

$$\hat{y}(r, s)=\sum_{n=0}^{2N-1}\sum_{m=0}^{2M-1}\hat{x}(n, m)\hat{h}[\langle r-n\rangle_{2N}, \langle s-m\rangle_{2M}]$$

$$\begin{pmatrix} r=0, 1, \cdots, 2N-1 \\ s=0, 1, \cdots, 2M-1 \end{pmatrix}, \tag{15}$$

则

$$y(r, s)=\hat{y}(r+N, s+M)$$

$$\begin{pmatrix} r=0, 1, \cdots, N-1 \\ s=0, 1, \cdots, M-1 \end{pmatrix}. \tag{16}$$

证明 当$r=0, 1, \cdots, N-1$; $s=0, 1, \cdots, M-1$时，由(13)有

$$\begin{aligned} &\hat{y}(r+N, s+M) \\ &=\sum_{n=0}^{2N-1}\sum_{m=0}^{2M-1}\hat{x}(n, m)\hat{h}[\langle r+N-n\rangle_{2N}, \langle s+M-m\rangle_{2M}] \\ &=\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}x(n, m)\hat{h}[\langle r+N-n\rangle_{2N}, \langle s+M-m\rangle_{2M}]. \end{aligned}$$

由于当 $r, n=0, 1, \cdots, N-1$; $s, m=0, 1, \cdots, M-1$ 时，有

$$1 \leqslant r+N-n \leqslant 2N-1,$$

$$1 \leqslant s+M-m \leqslant 2M-1.$$

由(14)式知

$$\hat{h}[\langle r+N-n\rangle_{2N}, \langle s+M-m\rangle_{2M}]$$
$$=\hat{h}(r+N-n, s+M-m)=h(r-n, s-m),$$

故有

$$\hat{y}(r+N, s+M)$$
$$=\sum_{n=0}^{N-1}\sum_{m=0}^{M-1} x(n, m)h(r-n, s-m)=y(r, s)$$
$$\begin{pmatrix} r=0, 1, \cdots, N-1 \\ s=0, 1, \cdots, M-1 \end{pmatrix}.$$

证毕.

由(13)和(14)，$(\hat{x})$ 和 $(\hat{h})$ 为:

$$(\hat{x})=\{\hat{x}(n, m)\}_{2N\times 2M}$$

$$=\overbrace{\begin{bmatrix} x(0, 0) & x(0, 1) & \cdots & x(0, M-1) & 0 & 0 & \cdots & 0 \\ x(1, 0) & x(1, 1) & \cdots & x(1, M-1) & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & & & & \vdots \\ x(N-1, 0) & x(N-1, 1) & \cdots & x(N-1, M-1) & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & & & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}}^{2M} \left.\vphantom{\begin{bmatrix}1\\1\\1\\1\\1\\1\\1\\1\end{bmatrix}}\right\} 2N. \tag{13'}$$

$$(\hat{h})=\{\hat{h}(n,\ m)\}_{2N\times 2M}$$

$$=\underbrace{\begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & h(-N+1,\ -M+1) & \cdots & h(-N+1,0) & h(-N+1,1) & \cdots & h(-N+1,M-1) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & h(0,\ -M+1) & \cdots & h(0,\ 0) & h(0,\ 1) & \cdots & h(0,\ M-1) \\ 0 & h(1,\ -M+1) & \cdots & h(1,\ 0) & h(1,\ 1) & \cdots & h(1,\ M-1) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & h(N-1,\ -M+1) & \cdots & h(N-1,\ 0) & h(N-1,\ 1) & \cdots & h(N-1,\ M-1) \end{bmatrix}}_{2M}\left.\vphantom{\begin{matrix}0\\0\\0\\0\\0\\0\\0\end{matrix}}\right\}2N \qquad (14')$$

$(\hat{y})$也是$2N\times 2M$数阵. 由(16)式知, $(\hat{y})$的右下角$N\times M$子数阵即为(y).

二、二维离散傅里叶变换

引理1和引理2分别将二维卷积和二维恒定对角卷积化作二维循环卷积. 二维循环卷积通常用变换法来计算. 最常用的是二维离散傅里叶变换.

二维 DFT 的定义是: 设$(x)=\{x(n, m)\}_{N\times M}$, 称

$$X(r, s)=\mathrm{DFT}(x)=\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}x(n, m)W_N^{rn}W_M^{sm} \tag{17}$$

$$\begin{pmatrix} r=0, 1, \cdots, N-1 \\ s=0, 1, \cdots, M-1 \end{pmatrix}$$

为二维 DFT. 其逆变换为

$$\begin{aligned} x(n, m)&=\mathrm{IDFT}(X) \\ &=\frac{1}{NM}\sum_{r=0}^{N-1}\sum_{s=0}^{M-1}X(r, s)W_N^{-rn}W_M^{-sm} \end{aligned} \tag{18}$$

$$\begin{pmatrix} n=0, 1, \cdots, N-1 \\ m=0, 1, \cdots, M-1 \end{pmatrix},$$

其中, $W_N=e^{-j\frac{2\pi}{N}}$, $W_M=e^{-j\frac{2\pi}{M}}$.

(17)和(18)的矩阵形式是:

$$(X)=(T_N)(x)(T_M), \tag{17'}$$

$$(x)=(T_N^{-1})(X)(T_M^{-1}), \tag{18'}$$

其中,

$$(x)=\begin{bmatrix} x(0, 0) & x(0, 1) & \cdots & x(0, M-1) \\ x(1, 0) & x(1, 1) & \cdots & x(1, M-1) \\ \vdots & \vdots & \vdots & \vdots \\ x(N-1, 0) & x(N-1, 1) & \cdots & x(N-1, M-1) \end{bmatrix},$$

$$(X)=\begin{bmatrix} X(0,0) & X(0,1) & \cdots & X(0,M-1) \\ X(1,0) & X(1,1) & \cdots & X(1,M-1) \\ \vdots & \vdots & \vdots & \vdots \\ X(N-1,0) & X(N-1,1) & \cdots & X(N-1,M-1) \end{bmatrix},$$

$$(T_N)=\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & W_N & \cdots & W_N^{N-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & W_N^{N-1} & \cdots & W_N^{(N-1)^2} \end{bmatrix},$$

$$(T_N^{-1})=\frac{1}{N}\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & W_N^{-1} & \cdots & W_N^{-(N-1)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & W_N^{-(N-1)} & \cdots & W_N^{-(N-1)^2} \end{bmatrix},$$

$$(T_M)=\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & W_M & \cdots & W_M^{M-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & W_M^{M-1} & \cdots & W_M^{(M-1)^2} \end{bmatrix},$$

$$(T_M^{-1})=\frac{1}{M}\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & W_M^{-1} & \cdots & W_M^{-(M-1)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & W_M^{-(M-1)} & \cdots & W_M^{-(M-1)^2} \end{bmatrix}.$$

这对变换最重要的性质是循环卷积特性.

设 $$X(r, s)=\mathrm{DFT}\{x(n, m)\},$$

$$H(r, s)=\mathrm{DFT}\{h(n, m)\},$$

$$Y(r, s)=\mathrm{DFT}\{y(n, m)\},$$

其中 $y(n, m)=\sum_{k=0}^{N-1}\sum_{l=0}^{M-1}x(k, l)h[\langle n-k\rangle_N, \langle m-l\rangle_M]$,

则

$$Y(r,\ s)=X(r,\ s)H(r,\ s)\ \begin{pmatrix} r=0,\ 1,\ \cdots,\ N-1 \\ s=0,\ 1,\ \cdots,\ M-1 \end{pmatrix}. \tag{19}$$

证明

$$\begin{aligned} Y(r,\ s)&=\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}y(n,\ m)W_N^{rn}W_M^{sm} \\ &=\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}\left[\sum_{l_1=0}^{N-1}\sum_{l_2=0}^{M-1}x(l_1,l_2)h[\langle n-l_1\rangle_N,\ \langle m-l_2\rangle_M]\right] \\ &\quad\times W_N^{rn}W_M^{sm}=\sum_{l_1=0}^{N-1}\sum_{l_2=0}^{M-1}\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}x(l_1,\ l_2) \\ &\quad\times h[\langle n-l_1\rangle_N,\ \langle m-l_2\rangle_M]W_N^{rn}W_M^{sm}, \end{aligned}$$

记 $n-l_1=k,\ m-l_2=l$，于是

$$\begin{aligned} Y(r,\ s)=&\sum_{l_1=0}^{N-1}\sum_{l_2=0}^{M-1}\sum_{k=-l_1}^{N-l_1-1}\sum_{l=-l_2}^{M-l_2-1}x(l_1,\ l_2)h[\langle k\rangle_N,\ \langle l\rangle_M] \\ &\times W_N^{r(l_1+k)}W_M^{s(l_2+l)}, \end{aligned}$$

由于 $\qquad h[\langle k+N\rangle_N,\ \ \langle l+M\rangle_M]=h[\langle k\rangle_N,\ \langle l\rangle_M],$

$$W_N^{n+N}=W_N^n,\quad W_M^{m+M}=W_M^m,$$

故有(参阅**5**中性质 3°)

$$\begin{aligned} Y(r,\ s)&=\sum_{l_1=0}^{N-1}\sum_{l_2=0}^{M-1}\sum_{k=0}^{N-1}\sum_{l=0}^{M-1}x(l_1,\ l_2)h(k,\ l)W_N^{rl_1}\cdot W_N^{sk} \\ &\quad\times W_M^{sl_2}\cdot W_M^{sl}=\sum_{l_1=0}^{N-1}\sum_{l_2=0}^{M-1}x(l_1,\ l_2)W_N^{rl_1}W_M^{sl_2} \\ &\quad\times\sum_{k=0}^{N-1}\sum_{l=0}^{M-1}h(k,\ l)W_N^{rk}\cdot W_M^{sl}=X(r,\ s)H(r,\ s) \\ &\qquad\begin{pmatrix} r=0,\ 1,\ \cdots,\ N-1 \\ s=0,\ 1,\ \cdots,\ M-1 \end{pmatrix}. \end{aligned}$$

证毕.

应用(19)式计算二维循环卷积时，共需要两次正变换、一次逆变换及 NM 次复数乘法. 一次 $N\times M$ 点的变换需要 $MN(M+N)$ 次复数乘法，所以利用(19)式计算 $N\times M$ 点的

循环卷积共需要 $3MN(N+M)+MN$ 次复数乘法. 若用快速算法(二维 FFT), 乘法次数可减少为 $NM(3\log_2 N+3\log_2 M+1)$.

例 1 求两数阵

$$(x)=\begin{bmatrix} 2 & 1 \\ -2 & 0 \end{bmatrix}, \qquad (h)=\begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}$$

的循环卷积.

【解】 先求 (x) 和 (h) 的二维 DFT. 由于

$$W_2=e^{-\frac{2\pi}{2}j}=-1,$$

故

$$(T_2)=\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \qquad (T_2^{-1})=\frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

$$\begin{aligned}(X)&=(T_2)(x)(T_2)\\ &=\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ -2 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}=\begin{bmatrix} 1 & -1 \\ 5 & 3 \end{bmatrix},\end{aligned}$$

$$(H)=(T_2)(h)(T_2)=\begin{bmatrix} 3 & 3 \\ -1 & -1 \end{bmatrix}.$$

利用二维 DFT 的循环卷积特性, 有

$$\begin{aligned}(Y)&=\begin{bmatrix} X(0,0)H(0,0) & X(0,1)H(0,1) \\ X(1,0)H(1,0) & X(1,1)H(1,1) \end{bmatrix}\\ &=\begin{bmatrix} 3 & -3 \\ -5 & -3 \end{bmatrix},\end{aligned}$$

将 (Y) 进行逆变换, 得

$$\begin{aligned}(y)&=(T_2^{-1})(Y)(T_2^{-1})\\ &=\frac{1}{4}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 3 & -3 \\ -5 & -3 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}=\begin{bmatrix} -2 & 1 \\ 2 & 2 \end{bmatrix}.\end{aligned}$$

故所给数阵的循环卷积是

$$(y)=\begin{bmatrix}-2 & 1\\ 2 & 2\end{bmatrix}.$$

例 2 求如下两数阵

$$(x)=\begin{bmatrix}2 & 1\\ -2 & 0\end{bmatrix},\qquad (h)=\begin{bmatrix}1 & 0\\ 2 & 0\end{bmatrix}$$

的二维卷积.

【解】 先用二维卷积的定义求. 由矩阵形式(5)得

$$\begin{bmatrix}y(0,0)\\ y(1,0)\end{bmatrix}=\begin{bmatrix}h(0,0) & 0\\ h(1,0) & h(0,0)\end{bmatrix}\begin{bmatrix}x(0,0)\\ x(1,0)\end{bmatrix}$$

$$=\begin{bmatrix}1 & 0\\ 2 & 1\end{bmatrix}\begin{bmatrix}2\\ -2\end{bmatrix}=\begin{bmatrix}2\\ 2\end{bmatrix},$$

$$\begin{bmatrix}y(0,1)\\ y(1,1)\end{bmatrix}=\begin{bmatrix}h(0,1) & 0\\ h(1,1) & h(0,1)\end{bmatrix}\begin{bmatrix}x(0,0)\\ x(1,0)\end{bmatrix}$$

$$+\begin{bmatrix}h(0,0) & 0\\ h(1,0) & h(0,0)\end{bmatrix}\begin{bmatrix}x(0,1)\\ x(1,1)\end{bmatrix}$$

$$=\begin{bmatrix}1 & 0\\ 2 & 1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix}=\begin{bmatrix}1\\ 2\end{bmatrix}.$$

故用定义求得所给数阵的二维卷积是

$$(y)=\begin{bmatrix}2 & 1\\ 2 & 2\end{bmatrix}.$$

下面再用二维 DFT 来计算.

由引理 1, 对 (x) 和 (h) 补零扩充成 4×4 数阵:

$$(\hat{x})=\left[\begin{array}{cc:cc}2 & 1 & 0 & 0\\ -2 & 0 & 0 & 0\\ \hdashline 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{array}\right],\qquad (\hat{h})=\left[\begin{array}{cc:cc}1 & 0 & 0 & 0\\ 2 & 0 & 0 & 0\\ \hdashline 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{array}\right],$$

求$(\hat{x})$和$(\hat{h})$的循环卷积$(\hat{y})$. 这可用二维 DFT 来求.

$$W_4=e^{-j\frac{2\pi}{4}}=-j,\quad W_4^{-1}=e^{j\frac{2\pi}{4}}=j,$$

故
$$(T_4)=\begin{bmatrix}1&1&1&1\\1&-j&-1&j\\1&-1&1&-1\\1&j&-1&-j\end{bmatrix},$$

$$(T_4^{-1})=\frac{1}{4}\begin{bmatrix}1&1&1&1\\1&j&-1&-j\\1&-1&1&-1\\1&-j&-1&j\end{bmatrix}.$$

$$(\hat{X})=(T_4)(\hat{x})(T_4)$$

$$=\begin{bmatrix}1&1&1&1\\1&-j&-1&j\\1&-1&1&-1\\1&j&-1&-j\end{bmatrix}\begin{bmatrix}2&1&0&0\\-2&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix}$$

$$\times\begin{bmatrix}1&1&1&1\\1&-j&-1&j\\1&-1&1&-1\\1&j&-1&-j\end{bmatrix}$$

$$=\begin{bmatrix}1&-j&-1&j\\3+2j&2+j&1+2j&2+3j\\5&4-j&3&4+j\\3-2j&2-3j&1-2j&2-j\end{bmatrix},$$

$$(\hat{H})=(T_4)(\hat{h})(T_4)$$

$$=\begin{bmatrix} 3 & 3 & 3 & 3 \\ 1-2j & 1-2j & 1-2j & 1-2j \\ -1 & -1 & -1 & -1 \\ 1+2j & 1+2j & 1+2j & 1+2j \end{bmatrix}.$$

因此

$$(\hat{Y})=\{\hat{X}(r,s)\hat{H}(r,s)\}$$

$$=\begin{bmatrix} 3 & -3j & -3 & 3j \\ 7-4j & 4-3j & 5 & 8-j \\ -5 & -4+j & -3 & -4-j \\ 7+4j & 8+j & 5 & 4+3j \end{bmatrix},$$

再求$(\hat{Y})$的逆变换，得

$$(\hat{y})=(T_4^{-1})(\hat{Y})(T_4^{-1})=\frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & j & -1 & -j \\ 1 & -1 & 1 & -1 \\ 1 & -j & -1 & j \end{bmatrix}$$

$$\times\begin{bmatrix} 3 & -3j & -3 & 3j \\ 7-4j & 4-3j & 5 & 8-j \\ -5 & -4+j & -3 & -4-j \\ 7+4j & 8+j & 5 & 4+3j \end{bmatrix}$$

$$\times\frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & j & -1 & -j \\ 1 & -1 & 1 & -1 \\ 1 & -j & -1 & j \end{bmatrix}=\begin{bmatrix} 2 & 1 & 0 & 0 \\ 2 & 2 & 0 & 0 \\ -4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

由引理 1，$(\hat{y})$左上角 2×2 子数阵即为(y)，故

$$(y)=\begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix}.$$

此即所给数阵的二维卷积，与定义求得的相同.

三、二维数论变换

类比于二维 DFT 及参照一维数论变换，可如下定义二维数论变换.

设 P 为正整数，以 P 为模的整数环为 Z_p:

$$Z_p=\{0,\ 1,\ 2,\ \cdots,\ P-1\}.$$

设 $x(n,\ m)\in Z_p(n=0,\ 1,\ \cdots,\ N-1;\ m=0,\ 1,\cdots,M-1)$，称

$$X(r,\ s)\equiv\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}x(n,\ m)\alpha^{rn}\beta^{sm}(\mathrm{mod}P)$$

$$\begin{pmatrix} r=0,\ 1,\ \cdots,\ N-1 \\ s=0,\ 1,\ \cdots,\ M-1 \end{pmatrix},\tag{20}$$

$$x(n,\ m)\equiv N^{-1}M^{-1}\sum_{r=0}^{N-1}\sum_{s=0}^{M-1}X(r,\ s)\alpha^{-rn}\beta^{-sm}(\mathrm{mod}P)$$

$$\begin{pmatrix} n=0,\ 1,\ \cdots,\ N-1 \\ m=0,\ 1,\ \cdots,\ M-1 \end{pmatrix}\tag{21}$$

为二维数论变换，其中，$\alpha\in Z_p$, $\beta\in Z_p$.

将(21)式代入(20)式，得到

$$X(r,\ s)\equiv\sum_{k=0}^{N-1}\sum_{l=0}^{M-1}X(k,\ l)\left[N^{-1}\sum_{n=0}^{N-1}\alpha^{n(r-k)}\right]$$

$$\times\left[M^{-1}\sum_{m=0}^{M-1}\beta^{m(s-l)}\right]\quad(\mathrm{mod}P).\tag{22}$$

因此，欲使(20)式与(21)式是一对互逆变换，必须且只需

$$N^{-1}\sum_{n=0}^{N-1}\alpha^{nj}\equiv\begin{cases}1, & j\equiv 0\quad(\mathrm{mod}N)\\ 0, & j\not\equiv 0\quad(\mathrm{mod}N)\end{cases}\quad(\mathrm{mod}P).\tag{23}$$

$$M^{-1}\sum_{m=0}^{M-1}\beta^{mi}\equiv\begin{cases}1, & i\equiv 0\quad(\mathrm{mod}M)\\ 0, & i\not\equiv 0\quad(\mathrm{mod}M)\end{cases}\quad(\mathrm{mod}P).\tag{24}$$

因此，我们可得到与一维数论变换相应的四个定理，其证明与一维数论变换完全相同.

定理 1 设 $P=p_1^{l_1}\cdot p_2^{l_2}\cdots p_s^{l_s}$，当且仅当

1° N^{-1} 和 M^{-1} 在 Z_p 上存在，即

$$(N, P)=1, \quad (M, P)=1;$$

2° α 对模 P 是 N 阶本原单位根，β 对模 P 是 M 阶本原单位根；

3° α 对模 $p_i(i=1, 2, \cdots, s)$ 的阶为 N，β 对模

$$p_i(i=1, 2, \cdots, s)$$

的阶是 M 时，(20) 与 (21) 是一对互逆变换. 当 P 是素数时，条件 2° 包含条件 3°.

定理 2 设 $P=p_1^{l_1}\cdot p_2^{l_2}\cdots p_s^{l_s}$，当且仅当

1° N^{-1} 与 M^{-1} 在 Z_p 上存在；

2° α 对模 $p_i^{l_i}(i=1, 2, \cdots, s)$ 的阶是 N，β 对模

$$p_i^{l_i}(i=1, 2, \cdots, s)$$

的阶是 M 时，(20) 与 (21) 是一对互逆变换.

定理 3 设 P 是自然数，当且仅当

1° N^{-1} 与 M^{-1} 在 Z_p 上存在；

2° α 对模 P 是 N 阶本原单位根，β 对模 P 是 M 阶本原单位根；

3° 存在 μ_j，$\nu_j \in Z_p$，使

$$\mu_j(\alpha^j-1)\equiv 1(j=1, 2, \cdots, N-1) \pmod{P},$$

$$\nu_j(\beta^j-1)\equiv 1(j=1, 2, \cdots, M-1) \pmod{P}$$

时，(20) 与 (21) 是一对互逆变换. 当 P 是素数时，条件 2° 包含条件 3°.

定理 4 设 $P=p_1^{l_1}\cdot p_2^{l_2}\cdots p_s^{l_s}$，(20) 与 (21) 构成一对互逆变换的充要条件是

$$N|O(P) \quad M|O(P).$$

定理 4 极为重要，它使我们可以具体地选择 N, M.

定理 5 在定理 1～4 的条件下，二维数论变换具有循环卷积特性.

这定理的证明与证明二维 DFT 的循环卷积特性完全相同，所不同是用 α 代替 W_N, β 代替 W_M.

推论 在整数环 Z_p 上，具有循环卷积特性的二维数论变换的最大长度是

$$N_{\max}=M_{\max}=O(P).$$

构成二维数论变换有五个参数：P, N, M, α, β. 取定 P, N, M, 可用 **6** 中的方法计算 α, β. 选取 P, N, M, α, β 的一般原则也如 **7** 中所述.

当模 P 取作 Mersenne 数 $M_q=2^q-1$, q 是素数时，称为二维 Mersenne 数变换. 这时可取:

$$\begin{cases} N=q \\ M=q \\ \alpha=2 \\ \beta=2, \end{cases} \qquad \begin{cases} N=2q \\ M=q \\ \alpha=-2 \\ \beta=2, \end{cases} \qquad \begin{cases} N=2q \\ M=2q \\ \alpha=-2 \\ \beta=-2. \end{cases}$$

当模 P 取作 Fermat 数 $F_t=2^b+1, b=2^t(t=1, 2, \cdots)$ 时，称为二维 Fermat 数变换. 这时可取:

$$\begin{cases} N=2b \\ M=2b \\ \alpha=2 \\ \beta=2, \end{cases} \qquad \begin{cases} N=4b \\ M=2b \\ \alpha=\sqrt{2} \\ \beta=2, \end{cases} \qquad \begin{cases} N=4b \\ M=4b \\ \alpha=\sqrt{2} \\ \beta=\sqrt{2}. \end{cases}$$

具体选法，可参阅表 3 .

二维数论变换的矩阵形式是

$$(X)\equiv(T_N)(x)(T_M) \pmod{P}, \tag{20'}$$

$$(x) \equiv (T_N^{-1})(X)(T_M^{-1}) \quad (\mathrm{mod} P), \qquad (21')$$

其中,

$$(x)=\begin{bmatrix} x(0,\ 0) & x(0,\ 1) & \cdots & x(0,\ M-1) \\ x(1,\ 0) & x(1,\ 1) & \cdots & x(1,\ M-1) \\ \vdots & \vdots & \vdots & \vdots \\ x(N-1,\ 0) & x(N-1,\ 1) & \cdots & x(N-1,\ M-1) \end{bmatrix},$$

$$(X)=\begin{bmatrix} X(0,0) & X(0,1) & \cdots & X(0,M-1) \\ X(1,0) & X(1,1) & \cdots & X(1,M-1) \\ \vdots & \vdots & \vdots & \vdots \\ X(N-1,0) & X(N-1,1) & \cdots & X(N-1,M-1) \end{bmatrix},$$

$$(T_N)\equiv\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{N-1} & \alpha^{2(N-1)} & \cdots & \alpha^{(N-1)^2} \end{bmatrix}(\mathrm{mod} P),$$

$$(T_N)\equiv N^{-1}\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(N-1)} \\ 1 & \alpha^{-2} & \alpha^{-4} & \cdots & \alpha^{-2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{-(N-1)} & \alpha^{-2(N-1)} & \cdots & \alpha^{-(N-1)^2} \end{bmatrix}(\mathrm{mod} P),$$

$$(T_M)\equiv\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \beta & \beta^2 & \cdots & \beta^{M-1} \\ 1 & \beta^2 & \beta^4 & \cdots & \beta^{2(M-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \beta^{M-1} & \beta^{2(M-1)} & \cdots & \beta^{(M-1)^2} \end{bmatrix}(\mathrm{mod} P),$$

$$(T_M^{-1}) \equiv M^{-1}\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \beta^{-1} & \beta^{-2} & \cdots & \beta^{-(M-1)} \\ 1 & \beta^{-2} & \beta^{-4} & \cdots & \beta^{-2(M-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \beta^{-(M-1)} & \beta^{-2(M-1)} & \cdots & \beta^{-(M-1)^2} \end{bmatrix} (\bmod P).$$

在用二维数论变换计算二维循环卷积时，模 P 必须满足

$$|y(r, s)| \leqslant \min\left\{|x(r, s)|_{\max}\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}|h(n, m)|,\right.$$

$$\left.|h(r, s)|_{\max}\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}|x(n, m)|\right\} < \frac{P}{2}$$

$$\begin{pmatrix} r=0, 1, \cdots, N-1 \\ s=0, 1, \cdots, M-1 \end{pmatrix}. \tag{25}$$

例 3 试用二维数论变换计算如下数阵

$$(x)=\begin{bmatrix} 2 & 1 & 0 & 0 \\ -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \qquad (h)=\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

的循环卷积

$$y(r, s)=\sum_{n=0}^{3}\sum_{m=0}^{3}x(n, m)h[\langle r-n\rangle_4, \langle s-m\rangle_4].$$

【解】 由于

$$|y(r, s)| \leqslant \sum_{n=0}^{3}\sum_{m=0}^{3}|x(n, m)|\,|h[\langle r-n\rangle_4, (s-m)_4]|$$

$$\leqslant |x(r, s)|_{\max}\sum_{n=0}^{3}\sum_{m=0}^{3}|h(n, m)|$$

$$\leqslant 2\cdot 4=8 \quad (r, s=0, 1, 2, 3),$$

根据(25)，必须 $8<\frac{P}{2}$. 取 $P=17$, $N=4$, $M=4$, $\alpha=4$, $\beta=4$. 这时，由于 $4^{-1}=-4$, 故

$$(T_4)\equiv\begin{bmatrix}1&1&1&1\\1&\alpha&\alpha^2&\alpha^3\\1&\alpha^2&\alpha^4&\alpha^6\\1&\alpha^3&\alpha^6&\alpha^9\end{bmatrix}\equiv\begin{bmatrix}1&1&1&1\\1&4&-1&-4\\1&-1&1&-1\\1&-4&-1&4\end{bmatrix}$$

$$\equiv\begin{bmatrix}1&1&1&1\\1&4&16&13\\1&16&1&16\\1&13&16&4\end{bmatrix}\quad(\text{mod}17),$$

$$(T_4^{-1})\equiv4^{-1}\begin{bmatrix}1&1&1&1\\1&\alpha^{-1}&\alpha^{-2}&\alpha^{-3}\\1&\alpha^{-2}&\alpha^{-4}&\alpha^{-6}\\1&\alpha^{-3}&\alpha^{-6}&\alpha^{-9}\end{bmatrix}$$

$$\equiv-4\begin{bmatrix}1&1&1&1\\1&-4&-1&4\\1&-1&1&-1\\1&4&-1&-4\end{bmatrix}$$

$$\equiv13\begin{bmatrix}1&1&1&1\\1&13&16&4\\1&16&1&16\\1&4&16&13\end{bmatrix}\quad(\text{mod}17).$$

于是

$$(X)\equiv(T_4)(x)(T_4)$$

$$\equiv\begin{bmatrix}1&4&-1&4\\-5&-2&-7&7\\5&8&3&0\\-6&-3&-8&6\end{bmatrix}\quad(\text{mod}17),$$

$$(H) \equiv (T_4)(h)(T_4)$$

$$\equiv \begin{bmatrix} 4 & 7 & 2 & -1 \\ -2 & -7 & 7 & -5 \\ 0 & -3 & 2 & 5 \\ -2 & 3 & 6 & 1 \end{bmatrix} \pmod{17}.$$

利用二维数论变换的循环卷积特性，有

$$(Y) \equiv \begin{bmatrix} 4 & 28 & -2 & -4 \\ 10 & 14 & -49 & -35 \\ 0 & -24 & 6 & 0 \\ 12 & -9 & -48 & 6 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 4 & -6 & -2 & -4 \\ -7 & -3 & 2 & -1 \\ 0 & -7 & 6 & 0 \\ -5 & 8 & 3 & 6 \end{bmatrix} \pmod{17}.$$

进行逆变换，得

$$(y) \equiv (T_4^{-1})(Y)(T_4^{-1})$$

$$\equiv \begin{bmatrix} -2 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 4 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \end{bmatrix} \pmod{17}.$$

取各项的绝对最小剩余，就得到所给数阵(x)和(h)的循环卷积值为：

$$(y) = \begin{bmatrix} -2 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 4 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \end{bmatrix}.$$

例 4 求数阵

$$(x)=\begin{bmatrix}1 & 2\\ 0 & -2\end{bmatrix},\qquad (h)=\begin{bmatrix}1 & 0\\ -1 & -2\end{bmatrix}$$

的二维卷积.

【解】 根据引理 1, 首先将 (x) 和 (h) 补零扩充成 4×4 数阵 $(\hat{x})$ 和 $(\hat{h})$:

$$(\hat{x})=\begin{bmatrix}1 & 2 & 0 & 0\\ 0 & -2 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{bmatrix},\qquad (\hat{h})=\begin{bmatrix}1 & 0 & 0 & 0\\ -1 & -2 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{bmatrix}.$$

求 $(\hat{x})$ 和 $(\hat{h})$ 的循环卷积 $(\hat{y})$, 其步骤与例 3 相同. 选取 $P=17$, $N=M=4$, $\alpha=\beta=4$, (T_4) 与 (T_4^{-1}) 如例 3 所示. 于是

$$(\hat{X})\equiv(T_4)(\hat{x})(T_4)$$

$$\equiv\begin{bmatrix}1 & 1 & 1 & 1\\ -5 & -6 & 7 & 8\\ 5 & 0 & -3 & 2\\ 6 & 7 & 8 & -5\end{bmatrix}\pmod{17},$$

$$(\hat{H})\equiv(T_4)(\hat{h})(T_4)$$

$$\equiv\begin{bmatrix}-2 & -8 & 2 & 8\\ 6 & -1 & 5 & -5\\ 4 & -7 & 0 & -6\\ -4 & 3 & -3 & 7\end{bmatrix}\pmod{17}.$$

从而 $$(\hat{Y})\equiv\begin{bmatrix}-2 & -8 & 2 & 8\\ 4 & 6 & 1 & -6\\ 3 & 0 & 0 & 5\\ 7 & 4 & -7 & -1\end{bmatrix}\pmod{17}.$$

利用逆变换得到

$$(\hat{y}) \equiv (T_4^{-1})(\hat{Y})(T_4^{-1})$$

$$\equiv \begin{bmatrix} 1 & 2 & 0 & 0 \\ -1 & -6 & -4 & 0 \\ -2 & -7 & 6 & -8 \\ 0 & 0 & 0 & 0 \end{bmatrix} \pmod{17}.$$

取各项的绝对最小剩余，就得到$(\hat{x})$和$(\hat{h})$的循环卷积的真值$(\hat{y})$：

$$(\hat{y}) = \begin{bmatrix} 1 & 2 & 0 & 0 \\ -1 & -6 & -4 & 0 \\ -2 & -7 & 6 & -8 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

根据引理1，取$(\hat{y})$的左上角2×2子数阵，就得到所给数阵(x)和(h)的二维卷积

$$(y) = \begin{bmatrix} 1 & 2 \\ -1 & -6 \end{bmatrix}.$$

四、多维卷积和多维数论变换

设两个K维数阵$x(n, m, \cdots, l)$，$h(n, m, \cdots, l)$ $(n=0, 1, \cdots, N-1; m=0, 1, \cdots, M-1; \cdots; l=0, 1, \cdots, L-1)$，称

$$y(r, s, \cdots, t) = \sum_{n=0}^{N-1}\sum_{m=0}^{M-1}\cdots\sum_{l=0}^{L-1} x(n, m, \cdots, l)h(r-n, s-m, \cdots, t-l)$$

$$\begin{pmatrix} r=0, 1, \cdots, N-1 \\ s=0, 1, \cdots, M-1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ t=0, 1, \cdots, L-1 \end{pmatrix} \tag{26}$$

为 K 维卷积，而称

$$y(r, s, \cdots, t)=\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}\cdots\sum_{l=0}^{L-1}x(n, m, \cdots, l)\times h[\langle r-n\rangle_N, \langle s-m\rangle_M, \cdots\langle t-l\rangle_L]$$

$$\begin{pmatrix} r=0, 1, \cdots, N-1 \\ s=0, 1, \cdots, M-1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ t=0, 1, \cdots, L-1 \end{pmatrix} \quad (27)$$

为 K 维循环卷积.

多维卷积可以和二维卷积那样，通过补零扩充，用多维循环卷积来计算，而多维循环卷积又可用如下的多维数论变换来实现.

设 P 为自然数，$x(n, m, \cdots, l)\in Z_p(n=0, 1, \cdots, N-1;$ $m=0, 1, \cdots, M-1; \cdots; l=0, 1, \cdots L-1)$，称如下一对变换

$$X(r, s, \cdots, t)\equiv\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}\cdots\sum_{l=0}^{L-1}x(n, m, \cdots, l)\alpha^{rn}\beta^{sm}\cdots\nu^{tl} \pmod{P}, \quad (28)$$

$$x(n, m, \cdots, l)\equiv N^{-1}M^{-1}\cdots L^{-1}\sum_{r=0}^{N-1}\sum_{s=0}^{M-1}\cdots\sum_{t=0}^{L-1}X(r, s, \cdots, t)\times\alpha^{-rn}\beta^{-sm}\cdots\nu^{-tl} \pmod{P} \quad (29)$$

为 K 维数论变换. 其中，$\alpha\in Z_p$, $\beta\in Z_p$, $\cdots$, $\nu\in Z_p$.

对于 K 维数论变换与二维数论变换一样，有如下定理:

定理 6 设 $P=p_1^{l_1}\cdot p_2^{l_2}\cdots p_s^{l_s}$，(28)与(29)是一对互逆变换的充要条件是:

1° N^{-1}, M^{-1}, $\cdots$, L^{-1} 在 Z_p 上存在;

2° α, β, $\cdots$, ν 对模 P 分别是 N 阶，M 阶，$\cdots$，L 阶本

原单位根;

3° $\alpha, \beta, \cdots, \nu$ 对模 $p_i(i=1, 2, \cdots, s)$ 的阶数分别是 $N, M, \cdots, L$.

定理 7 设 $P=p_1^{l_1}\cdot p_2^{l_2}\cdots p_s^{l_s}$, (28)和(29)是一对互逆变换的充要条件是

$$N|O(P), M|O(P), \cdots, L|O(P).$$

定理 8 在定理 6~8 的条件下，K 维数论变换(28)和(29)具有循环卷积特性.

在给定模 P 时, 在 Z_p 上具有循环卷积特性的 K 维数变换的最大长度是 $N_{max}=M_{max}=\cdots=L_{max}=O(P)$.

当 P 取作 Mersenne 数或 Fermat 数时，分别称为多维 Mersenne 数变换及多维 Fermat 数变换.

—14—

减少字长的几种考虑

上节我们讨论了二维卷积及二维数论变换. 现在回过头来考虑一维卷积.

前面已经讲过,用一维数论变换(如 FNT)去实现长序列的变换或卷积时,需要较大的字长. 我们在这一节就要研究如何用较短的字长去实现长序列的卷积. 这里我们介绍两个方法. 一个是一维卷积多维处理. 这个方法是把一维循环卷积化为二维或多维循环卷积,再用二维或多维数论变换去实现这个二维或多维循环卷积,从而达到减少字长的目的. 另一个是分段处理法,将长序列的卷积分作若干段,每一段是一些短序列的卷积,它们都可用较短字长的变换去处理,这样也能达到减少字长的目的.

一、一维循环卷积化作二维循环卷积的方法

设两个长为 N 的序列 $x(n)$ 和 $h(n)$ $(n=0,1,\cdots,N-1)$,其循环卷积为

$$y(n)=\sum_{q=0}^{N-1}x(q)h[\langle n-q\rangle_N]\quad (n=0,\ 1,\ \cdots,\ N-1).\tag{1}$$

设

$$N=L\cdot M\quad (L>1,\ M>1,\ \text{皆为正整数}),\tag{2}$$

作置换

$$\begin{matrix}n=l+mL\\ q=k+pL\end{matrix}\begin{pmatrix}k,\ l=0,\ 1,\ \cdots,\ L-1\\ m,\ p=0,\ 1,\ \cdots,\ M-1\end{pmatrix},\tag{3}$$

于是(1)式成为

$$y(l+mL)=\sum_{k=0}^{L-1}\sum_{p=0}^{M-1}x(k+pL)$$

$$\times h[\langle(l-k)+L(m-p)\rangle_N]. \tag{4}$$

记

$$x(l+mL)=\hat{x}(l,\ m)$$

$$y(l+mL)=\hat{y}(l,\ m)$$

$$h[\langle l+mL\rangle_N]=\hat{h}(l,\ m)$$

$$\begin{pmatrix} l=0,\ 1,\ \cdots,\ L-1 \\ m=0,\ 1,\ \cdots,\ M-1 \end{pmatrix}, \tag{5}$$

那么，(4)式就形式上成为

$$\hat{y}(l,\ m)=\sum_{k=0}^{L-1}\sum_{p=0}^{M-1}\hat{x}(k,\ p)\hat{h}(l-k,\ m-p). \tag{6}$$

(6)式是一种二维卷积，但是(6)式中的 $\hat{h}(l-k,\ m-p)$ 要超出(5)式定义的范围．事实上，当 $k,\ l=0,\ 1,\ \cdots,\ L-1$; $m,\ p=0,\ 1,\cdots,\ M-1$ 时，有

$$-(L-1)\leqslant l-k\leqslant L-1,$$

$$-(M-1)\leqslant m-p\leqslant M-1.$$

考虑到(1)式是循环卷积，$h[\langle k\rangle_N]$ 对一切整数 k 均有定义，故(5)式可改写作：

$$\hat{y}(l,\ m)=y(l+mL)$$

$$\hat{x}(l,\ m)=x(l+mL)$$

$$\begin{pmatrix} l=0,\ 1,\ \cdots,\ L-1 \\ m=0,\ 1,\ \cdots,\ M-1 \end{pmatrix},$$

$$\hat{h}(r,\ s)=h[\langle r+sL\rangle_N] \tag{7}$$

$$\begin{pmatrix} -(L-1)\leqslant r\leqslant L-1 \\ -(M-1)\leqslant s\leqslant M-1 \end{pmatrix}.$$

这样(4)式就成为如下二维卷积：

$$\hat{y}(l,\ m)=\sum_{k=0}^{N-1}\sum_{p=0}^{M-1}\hat{x}(k,\ p)\hat{h}(l-k,\ m-p). \tag{8}$$

引理 1 如果 $\hat{h}(r,\ s)$ 由(7)式定义，则

$$\hat{h}(r,\ s+M)=\hat{h}(r,\ s).$$

事实上，

$$\begin{aligned}\hat{h}(r,\ s+M)&=h[\langle r+L(s+M)\rangle_N]\\&=h[\langle r+sL+ML\rangle_N]\\&=h[\langle r+sL\rangle_N]=\hat{h}(r,\ s).\end{aligned} \tag{9}$$

这个引理表示，(8)式对第二维 p 是循环卷积，而对第一维 k 却不是循环的，故可记作：

$$\hat{y}(l,\ m)=\sum_{k=0}^{L-1}\sum_{p=0}^{M-1}\hat{x}(k,\ p)\hat{h}[l-k,\ \langle m-p\rangle_M], \tag{10}$$

式(10)中的二维数阵 $(\hat{x})$ 和 $(\hat{h})$，$(\hat{y})$ 分别为

$$(\hat{x})=\begin{bmatrix}\hat{x}(0,\ 0) & \hat{x}(0,\ 1) & \cdots & \hat{x}(0,\ M-1)\\ \hat{x}(1,\ 0) & \hat{x}(1,\ 1) & \cdots & \hat{x}(1,\ M-1)\\ \vdots & \vdots & \vdots & \vdots\\ \hat{x}(L-1,\ 0) & \hat{x}(L-1,\ 1) & \cdots & \hat{x}(L-1,\ M-1)\end{bmatrix}$$

$$=\left.\overbrace{\begin{bmatrix}x(0) & x(L) & \cdots & x(N-L)\\ x(1) & x(L+1) & \cdots & x(N-L+1)\\ \vdots & \vdots & \vdots & \vdots\\ x(L-1) & x(2L-1) & \cdots & x(N-1)\end{bmatrix}}^{M},\ \right\}L \tag{11}$$

$$(\hat{y})=\begin{bmatrix}\hat{y}(0,\ 0) & \hat{y}(0,\ 1) & \cdots & \hat{y}(0,\ M-1)\\ \hat{y}(1,\ 0) & \hat{y}(1,\ 1) & \cdots & \hat{y}(1,\ M-1)\\ \vdots & \vdots & \vdots & \vdots\\ \hat{y}(L-1,\ 0) & \hat{y}(L-1,\ 1) & \cdots & \hat{y}(L-1,\ M-1)\end{bmatrix}$$

$$
= \overbrace{\begin{bmatrix} y(0) & y(L) & \cdots & y(N-L) \\ y(1) & y(L+1) & \cdots & y(N-L+1) \\ \vdots & \vdots & \vdots & \vdots \\ y(L-1) & y(2L-1) & \cdots & y(N-1) \end{bmatrix}}^{M}, \Bigg\} L
$$

$$
(\hat{h})
$$

$$
= \begin{bmatrix} \hat{h}(-L+1,\ 0) & \hat{h}(-L+1,\ 1) & \cdots & \hat{h}(-L+1,\ M-1) \\ \hat{h}(-L+2,\ 0) & \hat{h}(-L+2,\ 1) & \cdots & \hat{h}(-L+2,\ M-1) \\ \vdots & \vdots & \vdots & \vdots \\ \hat{h}(0,\ 0) & \hat{h}(0,\ 1) & \cdots & \hat{h}(0,\ M-1) \\ \hat{h}(1,\ 0) & \hat{h}(1,\ 1) & \cdots & \hat{h}(1,\ M-1) \\ \vdots & \vdots & \vdots & \vdots \\ \hat{h}(L-1,\ 0) & \hat{h}(L-1,\ 1) & \cdots & \hat{h}(L-1,\ M-1) \end{bmatrix}
$$

$$
= \overbrace{\begin{bmatrix} h(N-L+1) & h(1) & \cdots & h(N-2L+1) \\ h(N-L+2) & h(2) & \cdots & h(N-2L+2) \\ \vdots & \vdots & \vdots & \vdots \\ h(0) & h(L) & \cdots & h(N-L) \\ h(1) & h(L+1) & \cdots & h(N-L+1) \\ \vdots & \vdots & \vdots & \vdots \\ h(L-1) & h(2L-1) & \cdots & h(N-1) \end{bmatrix}}^{M}. \Bigg\} 2L-1 \tag{11'}
$$

下面我们要将(10)式化为二维循环卷积来计算. 象(10)式这种卷积就是 **13** 中考虑过的二维恒定对角卷积的特殊情况.

引理 2 设$(\hat{x})$和$(\hat{h})$如(11)式和(11')式所示，卷积(10)式可通过如下的$2L\times M$数阵$(\hat{\hat{x}})$和$(\hat{\hat{h}})$的二维循环卷积来计算.

设

$$\hat{\hat{x}}(l,\ m)=\begin{cases}\hat{x}(l,\ m)\begin{pmatrix} l=0,\ 1,\ \cdots,\ N-1 \\ m=0,\ 1,\ \cdots,\ M-1\end{pmatrix}, \\ 0, \qquad\qquad \text{其它};\end{cases} \tag{12}$$

$$\hat{\hat{h}}(l,\ m)=\begin{cases}0 \quad (l=0,\ m=0,\ 1,\ \cdots,\ M-1), \\ \hat{h}(-L+l,\ m)\begin{pmatrix} l=1,\ 2,\ \cdots,\ 2L-1 \\ m=0,\ 1,\ \cdots,\ M-1\end{pmatrix}.\end{cases} \tag{13}$$

作$(\hat{\hat{x}})$和$(\hat{\hat{h}})$的循环卷积

$$\hat{\hat{y}}(l,\ m)=\sum_{k=0}^{2L-1}\sum_{p=0}^{M-1}\hat{\hat{x}}(k,\ p)\hat{\hat{h}}[\langle l-k\rangle_{2L},\ \langle m-p\rangle_{M}] \tag{14}$$

$$\begin{pmatrix} l=0,\ 1,\ \cdots,\ 2L-1 \\ m=0,\ 1,\ \cdots,\ M-1\end{pmatrix},$$

那么有

$$\hat{\hat{y}}(l+L,\ m)=y(l,\ m)\begin{pmatrix} l=0,\ 1,\ \cdots,\ L-1 \\ m=0,\ 1,\ \cdots,\ M-1\end{pmatrix}. \tag{15}$$

此引理的证明与 **13** 中引理 2 的证明相同.

(12)式和(13)式可用数阵表示为:

$$(\hat{\hat{x}})=\{\hat{\hat{x}}(l,\ m)\}_{2L\times M}$$

$$=\left.\begin{bmatrix} \overbrace{\begin{matrix} x(0) & x(L) & x(2L) & \cdots & x(N-L) \end{matrix}}^{M} \\ \begin{matrix} x(1) & x(L+1) & x(2L+1) & \cdots & x(N-L+1) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x(L-1) & x(2L-1) & x(3L-1) & \cdots & x(N-1) \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{matrix}\end{bmatrix},\right\}2L \tag{16}$$

$$(\hat{h})=\{\hat{h}(l,m)\}_{2L\times M}$$

$$=\overbrace{\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ h(N-L+1) & h(1) & h(L+1) & \cdots & h(N-2L+1) \\ h(N-L+2) & h(2) & h(L+2) & \cdots & h(N-2L+2) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ h(0) & h(L) & h(2L) & \cdots & h(N-L) \\ h(1) & h(L+1) & h(2L+1) & \cdots & h(N-L+1) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ h(L-1) & h(2L-1) & h(3L-1) & \cdots & h(N-1) \end{bmatrix}}^{M}.\Bigg\}2L \quad (17)$$

引理2就是一维循环卷积化为二维循环卷积的方法．从(16)式及(17)式看到，数阵$(\hat{x})$和$(\hat{h})$的元素都是用原来序列$\{x(n)\}$和$\{h(n)\}$的元素表示的．为了看得更清楚起见，举一例说明之．例如当$N=16$时，$x(n)$，$h(n)$ $(n=0,1,\cdots,15)$已经给定，要求它们的循环卷积$y(n)$ $(n=0,1,\cdots,15)$．按照引理2，由于$N=4\times4$，故可取$L=M=4$，这时$(\hat{x})$和$(\hat{h})$分别为：

$$(\hat{x})=\begin{bmatrix} x(0) & x(4) & x(8) & x(12) \\ x(1) & x(5) & x(9) & x(13) \\ x(2) & x(6) & x(10) & x(14) \\ x(3) & x(7) & x(11) & x(15) \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

$$(\hat{h})=\begin{bmatrix} 0 & 0 & 0 & 0 \\ h(13) & h(1) & h(5) & h(9) \\ h(14) & h(2) & h(6) & h(10) \\ h(15) & h(3) & h(7) & h(11) \\ h(0) & h(4) & h(8) & h(12) \\ h(1) & h(5) & h(9) & h(13) \\ h(2) & h(6) & h(10) & h(14) \\ h(3) & h(7) & h(11) & h(15) \end{bmatrix}.$$

求$(\hat{x})$和$(\hat{h})$的二维循环卷积$(\hat{\hat{y}})$，再取数阵$(\hat{\hat{y}})$下方 $L\times M$ 子数阵就得到$(\hat{y})$. 将数阵$(\hat{y})$的元素按列排列成一列矢量，就得到原来两个序列的循环卷积值$\{y(n)\}$. 下面举一具体例子说明这个方法.

例 1 一维卷积化为二维循环卷积的方法.

这个方法可以分作两步，第一步应用**1**中的引理1，将所给的一维卷积化作一维循环卷积；第二步再应用本节所述的方法将得到的一维循环卷积化为二维循环卷积. 具体的例子如下：

求两序列

$$(x)=\begin{bmatrix}2\\-2\\1\\0\end{bmatrix},\qquad (h)=\begin{bmatrix}2\\1\\0\\0\end{bmatrix}$$

的卷积 $$y_n=\sum_{k=0}^{3}x_k h_{\langle n-k\rangle_4}\qquad (n=0,\ 1,\ 2,\ 3).$$

【解】 根据**1**中的引理1，对所给序列(x)和(h)补零扩充作

$$(\hat{x})=\begin{bmatrix}2\\-2\\1\\0\\0\\0\\0\\0\end{bmatrix},\qquad (\hat{h})=\begin{bmatrix}2\\1\\0\\0\\0\\0\\0\\0\end{bmatrix}.$$

$(\hat{x})$和$(\hat{h})$的循环卷积是

$$\hat{y}_n=\sum_{k=0}^{7}\hat{x}_k\hat{h}_{\langle n-k\rangle_8}\quad (n=0,\ 1,\ \cdots,\ 7).$$

用本节所述的方法将它化为二维循环卷积. 这时 $N=8=2\cdot4$, 取 $L=2$, $M=4$. 由(16)和(17), $(\hat{\hat{x}})$ 和 $(\hat{\hat{h}})$ 分别为

$$(\hat{\hat{x}})=\begin{bmatrix}\hat{x}_0 & \hat{x}_2 & \hat{x}_4 & \hat{x}_6\\ \hat{x}_1 & \hat{x}_3 & \hat{x}_5 & \hat{x}_7\\ 0&0&0&0\\ 0&0&0&0\end{bmatrix}=\begin{bmatrix}2&1&0&0\\ -2&0&0&0\\ 0&0&0&0\\ 0&0&0&0\end{bmatrix},$$

$$(\hat{\hat{h}})=\begin{bmatrix}0&0&0&0\\ \hat{h}_7 & \hat{h}_1 & \hat{h}_3 & \hat{h}_5\\ \hat{h}_0 & \hat{h}_2 & \hat{h}_4 & \hat{h}_6\\ \hat{h}_1 & \hat{h}_3 & \hat{h}_5 & \hat{h}_7\end{bmatrix}=\begin{bmatrix}0&0&0&0\\ 0&1&0&0\\ 2&0&0&0\\ 1&0&0&0\end{bmatrix}.$$

用二维 FNT 求 $(\hat{\hat{x}})$ 和 $(\hat{\hat{h}})$ 的二维循环卷积 $(\hat{\hat{y}})$. 由 **13** 中的例 3, 得到*

$$(\hat{\hat{y}})=\begin{bmatrix}-2&0&0&0\\ 0&2&1&0\\ 4&0&0&0\\ -2&1&0&0\end{bmatrix}.$$

由本节引理 2 知,

$$(\hat{y})=\begin{bmatrix}4\\ -2\\ 0\\ 1\\ 0\\ 0\\ 0\\ 0\end{bmatrix}.$$

---

* $(\hat{\hat{y}})$ 的第一、二行元素实际不需要计算, 只需计算后面两行的元素, 这样可以节省一半计算量.

因此，所给序列(x)和(h)的一维卷积为

$$(y)=\begin{bmatrix}4\\-2\\0\\1\end{bmatrix}.$$

以上所述就是一维卷积二维处理的方案.根据这个方案，长度为$N=L\cdot M$的一维循环卷积是用$2L\times M$二维循环卷积来计算，而二维循环卷积用二维 FNT 来实现. 因此，当用$P=2^b+1$, $b=2^t$, $\alpha=\beta=2$, $2L=2b$, $M=2b$, 可以计算的一维循环卷积的长度是$L\cdot M=2b^2=N$, 当$\alpha=\beta=\sqrt{2}$, $2L=4b$, $M=4b$, 可计算的长度就为$8b^2=N$. 也就是说，一维卷积二维处理，所需的字长b与N的平方根成正比，或者说，用字长b可处理长度为与b^2成正比的一维循环卷积. 具体情况如表9所示. 如果所需计算的是一维卷积，那么表9所列的长度将减半.

表9 用二维 FNT 可得到的一维循环卷积的长度

$P=2^b+1$	字长 $b=2^t$	$\alpha=\beta=2$ $N=2b^2$	$\alpha=2,\ \beta=\sqrt{2}$ $N=4b^2$	$\alpha=\beta=\sqrt{2}$ $N=8b^2$
2^8+1	8	128	256	512
$2^{16}+1$	16	512	1024	2048
$2^{32}+1$	32	2048	4096	8192
$2^{64}+1$	64	8192	16384	32768

应用上述的一维卷积二维处理的思想，不难将一维卷积化作多维循环卷积来处理.

设 $N=\overbrace{L\cdot M\cdots R}^{S}$ $(L>1,\ M>1,\ \cdots,\ R>1$皆为正整数)，那么(1)式就成为$S$维卷积

$$\hat{y}(l, m, \cdots, r)=\sum_{n_1=0}^{L-1}\sum_{n_2=0}^{M-1}\cdots\sum_{n_s=0}^{R-1}\hat{x}(n_1, n_2, \cdots, n_s)$$
$$\times\hat{h}[l-n_1, l_2-n_2, \cdots, \langle r-n_s\rangle_R], \quad (18)$$

其中，
$$\hat{x}(l, m, \cdots, r)=x(l+mL+\cdots+r\cdot L\cdot M\cdots)$$
$$\hat{y}(l, m, \cdots, r)=y(l+mL+\cdots+r\cdot L\cdot M\cdots)$$
$$\left(\begin{array}{c} l=0, 1, \cdots, L-1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ r=0, 1, \cdots, R-1 \end{array}\right),$$
$$\hat{h}(l, m, \cdots, r)=h[\langle l+mL+\cdots+rL\cdot M\cdots\rangle_N]$$
$$\left(\begin{array}{c} -(L-1)\leqslant l\leqslant L-1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ -(R-1)\leqslant r\leqslant R-1 \end{array}\right).$$

特别，当 $N=2^s$ 时，取 $L=M=\cdots=R=2$，则(18)式就成为

$$\hat{y}(l, m, \cdots, r)=\sum_{n_1=0}^{1}\sum_{n_2=0}^{1}\cdots\sum_{n_s=0}^{1}\hat{x}(n_1, n_2, \cdots, n_s)$$
$$\times\hat{h}[l-n_1, m-n_2, \cdots, \langle r-n_s\rangle_2], \quad (19)$$

其中，
$$\hat{x}(l, m, \cdots, r)=x(l+2m+\cdots+2^{s-1}r)$$
$$\hat{y}(l, m, \cdots, r)=y(l+2m+\cdots+2^{s-1}r)$$
$$(l, m, \cdots, r=0, 1),$$
$$\hat{h}(l, m, \cdots, r)=\hat{h}[\langle l+2m+\cdots+2^{s-1}r\rangle_N]$$
$$(l, m, \cdots, r=-1, 0, 1).$$

(19)式为 S 维卷积，每维的长度是2. 可用各种算法计算(19)式.

如果欲用变换法计算(18)式，那么还需将(18)式化为 S 维循环卷积，这可仿二维处理情况，对$(\hat{x})$及$(\hat{h})$适当补零而成为$(\hat{\hat{x}})$，$(\hat{\hat{h}})$，再作$(\hat{\hat{x}})$，$(\hat{\hat{h}})$的 S 维循环卷积$(\hat{\hat{y}})$：

$$\hat{\hat{y}}(l, m, \cdots, r)=\sum_{n_1=0}^{2L-1}\sum_{n_2=0}^{2M-1}\cdots\sum_{n_s=0}^{R-1}\hat{\hat{x}}(n_1, n_2, \cdots, n_s)$$
$$\times\hat{\hat{h}}[\langle l-n_1\rangle_{2L}, \cdots, \langle r-n_s\rangle_R]. \quad (20)$$

(20)式可用 S 维数论变换计算. 计算出$(\hat{\hat{y}})$后, 再取$(\hat{\hat{y}})$的下半部 $L\times M\times\cdots\times R$ 子数阵,就得到$(\hat{y})$,从而得到(y).

一维卷积 S 维处理,是将长度为 $N=L\cdot M\cdots R$ 的一维循环卷积化作 $2L\times 2M\times\cdots\times R$ 的 S 维循环卷积来计算的, S 维循环卷积用 S 维 FNT 实现. 因此, 只需用 $b\propto N^{\frac{1}{s}}$的字长便能实现这个卷积. 也就是说, 用 b 位字长可处理的一维卷积的长度 N 与 b^s 成正比.

因此,一维卷积多维处理可减少字长. 当然,字长的减少必须与溢出的问题结合起来考虑. 一般地说, 一维卷积二维处理,较为理想.

二、分段处理

另一种用较短的字长处理较长序列卷积的方法是分段处理法. 这种方法是利用矩阵的分块相乘法将较长的卷积分成若干段,每一段分别加以处理. 为了叙述方便, 以 $N=8$ 加以说明.

设 $\{x_n\}$ 和 $\{h_n\}$ 是长为 $N=8$ 的序列,其卷积为

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} h_0 & & & & & & & \\ h_1 & h_0 & & & & \text{\Large 0} & & \\ h_2 & h_1 & h_0 & & & & & \\ h_3 & h_2 & h_1 & h_0 & & & & \\ h_4 & h_3 & h_2 & h_1 & h_0 & & & \\ h_5 & h_4 & h_3 & h_2 & h_1 & h_0 & & \\ h_6 & h_5 & h_4 & h_3 & h_2 & h_1 & h_0 & \\ h_7 & h_6 & h_5 & h_4 & h_3 & h_2 & h_1 & h_0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix}. \tag{21}$$

将(21)式分成 2×2 子矩阵，利用矩阵分块相乘法，得

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \begin{bmatrix} h_0 & 0 \\ h_1 & h_0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix},$$

$$\begin{bmatrix} y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} h_2 & h_1 \\ h_3 & h_2 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} h_0 & 0 \\ h_1 & h_0 \end{bmatrix} \begin{bmatrix} x_2 \\ x_3 \end{bmatrix},$$

$$\begin{bmatrix} y_4 \\ y_5 \end{bmatrix} = \begin{bmatrix} h_4 & h_3 \\ h_5 & h_4 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} h_2 & h_1 \\ h_3 & h_2 \end{bmatrix} \begin{bmatrix} x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} h_0 & 0 \\ h_1 & h_0 \end{bmatrix} \begin{bmatrix} x_4 \\ x_5 \end{bmatrix},$$

$$\begin{bmatrix} y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} h_6 & h_5 \\ h_7 & h_6 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} h_4 & h_3 \\ h_5 & h_4 \end{bmatrix} \begin{bmatrix} x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} h_2 & h_1 \\ h_3 & h_2 \end{bmatrix} \begin{bmatrix} x_4 \\ x_5 \end{bmatrix} + \begin{bmatrix} h_0 & 0 \\ h_1 & h_0 \end{bmatrix} \begin{bmatrix} x_6 \\ x_7 \end{bmatrix}. \tag{22}$$

也可以将(21)分成 4×4 矩阵：

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} h_0 & & & \\ h_1 & h_0 & & \\ h_2 & h_1 & h_0 & \\ h_3 & h_2 & h_1 & h_0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix},$$

$$\begin{bmatrix} y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} h_4 & h_3 & h_2 & h_1 \\ h_5 & h_4 & h_3 & h_2 \\ h_6 & h_5 & h_4 & h_3 \\ h_7 & h_6 & h_5 & h_4 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} h_0 & & & \\ h_1 & h_0 & & \\ h_2 & h_1 & h_0 & \\ h_3 & h_2 & h_1 & h_0 \end{bmatrix} \begin{bmatrix} x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix}. \tag{23}$$

出现于(22)及(23)式右端的子卷积有两种，一种是一般的一维卷积，另一种是恒定对角卷积(如果将(23)式中的 h_4 看作 **1** 中恒定对角卷积(6)的 h_0, 就完全相同). 这两种卷积已在 **1** 中考虑过如何将它们化为一维循环卷积，从而可用变换法计算.

由于可用上述方法将长序列卷积分成若干组短卷积，每一个短卷积可用较短的字长实现，这样就达到了用较短的字长实现较长序列卷积的计算目的. 具体应用这个方法时，首先根据溢出的考虑，确定模 M, 从而定下字长(16, 32, 64 及其它)，选定 α(2 或 $\sqrt{2}$ 或 2 的幂). 再根据表 3, 确定变换长度 N, 用 $\frac{N}{2}$ 将所给长卷积分成若干段，每一个子卷积便能用参数是 M, N, α 的 FNT 来实现. 这种方法实质上和二维处理法没有什么不同，可以看作二维处理的一种形式，但它简单、明了，如果适当设计，计算卷积的速度将比二维处理法快.

可能还有其它的方法，如对数据按高、低位分开处理，以减少字长. 这里不再叙述，读者可参阅文献[2].

—15—

数论变换的其它应用

数论变换的主要应用是计算两个序列的卷积．在数字信号处理(如在雷达、物探及医学技术等方面)中，卷积是非常有用的运算．本书前面各节详细的叙述了应用数论变换实现一维及二维卷积的计算．这里，我们简要的介绍数论变换在其它方面的应用．

一、应用复数数论变换计算序列的离散傅里叶变换

设 $\{x_n\}=(x_0,\ x_1,\ \cdots,\ x_{N-1})$ 是以 N 为周期的周期序列(N 是偶数)，记 $W_N=e^{-j\frac{2\pi}{N}}$，则 $\{x_n\}$ 的 DFT 是

$$X_k=\sum_{n=0}^{N-1}x_nW_N^{nk}\quad(k=0,\ 1,\ \cdots,\ N-1),\tag{1}$$

IDFT 是

$$x_n=\frac{1}{N}\sum_{k=0}^{N-1}X_kW_N^{-nk}\quad(n=0,\ 1,\ \cdots,\ N-1).\tag{2}$$

将(1)式改写作：

$$\begin{aligned}X_k&=\sum_{n=0}^{N-1}x_nW_N^{nk}=\sum_{n=0}^{N-1}x_n\,(W_N^{\frac{1}{2}})^{2nk}\\&=(W_N^{\frac{1}{2}})^{k^2}\sum_{n=0}^{N-1}(x_nW_N^{\frac{1}{2}n^2})W_N^{-\frac{(k-n)^2}{2}}\\&=(W_N^{\frac{1}{2}})^{k^2}\sum_{n=0}^{N-1}d_ng_{k-n}=(W_N^{\frac{1}{2}})^{k^2}y_k\\&\qquad(k=0,\ 1,\ \cdots,\ N-1),\end{aligned}\tag{3}$$

其中,

$$d_n = x_n W_N^{\frac{1}{2}n^2} \qquad (n=0,\ 1,\ \cdots,\ N-1), \tag{4}$$

$$g_n = W_N^{-\frac{1}{2}n^2}$$

$$y_k = \sum_{n=0}^{N-1} d_n g_{k-n} \quad (k=0,\ 1,\ \cdots,\ N-1). \tag{5}$$

由于 N 是偶数, 故 $d_{n+N}=d_n$, $g_{n+N}=g_n$, 这表示(5)式是循环卷积. 利用复数数论变换可以计算$\{y_k\}$, 再分别乘以 $W_N^{\frac{1}{2}k^2}$, 就得到 $\{X_k\}$.

同样将(2)式改写作:

$$x_n = \frac{1}{N}\sum_{k=0}^{N-1} X_k W_N^{-nk}$$

$$= \frac{1}{N}\sum_{k=0}^{N-1} X_k (W_N^{-\frac{1}{2}})^{k^2} \cdot (W_N^{-\frac{1}{2}})^{n^2} \cdot W_N^{\frac{1}{2}(k-n)^2}$$

$$= \frac{1}{N} W_N^{-\frac{1}{2}n^2} \sum_{k=0}^{N-1} (X_k W_N^{-\frac{1}{2}k^2}) W_N^{\frac{1}{2}(k-n)^2}$$

$$= \frac{1}{N} W_N^{-\frac{1}{2}n^2} \sum_{k=0}^{N-1} d'_k g'_{n-k}$$

$$= \frac{1}{N} W_N^{-\frac{1}{2}n^2} y'_n \quad (n=0,\ 1,\ \cdots,\ N-1), \tag{6}$$

其中,

$$d'_k = X_k W_N^{-\frac{1}{2}k^2} \qquad (k=0,\ 1,\ \cdots,\ N-1), \tag{7}$$

$$g'_k = W_N^{\frac{1}{2}k^2}$$

$$y'_n = \sum_{k=0}^{N-1} d'_k g'_{n-k} \quad (n=0,\ 1,\ \cdots,\ N-1). \tag{8}$$

由于 N 是偶数, $d'_{k+N}=d'_k$, $g'_{k+N}=g'_k$, 故(8)式是循环卷积, 可以用复数数论变换计算 $\{y'_n\}$, 从而得到 $\{x_n\}$.

例 1 设

$$\{x_n\}=\begin{bmatrix}x_0\\x_1\\x_2\\x_3\end{bmatrix}=\begin{bmatrix}1\\1\\1\\1\end{bmatrix},$$

试利用复数数论变换求其 DFT.

【解】

$$W_4=e^{-j\frac{2\pi}{4}}=e^{-j\frac{\pi}{2}},$$

$$W_4^{\frac{1}{2}}=e^{-j\frac{\pi}{4}}\approx 0.7-0.7j.$$

由(4)式，有

$$\begin{bmatrix}d_0\\d_1\\d_2\\d_3\end{bmatrix}=\begin{bmatrix}1\\0.7-j0.7\\-1\\0.7-j0.7\end{bmatrix}=\frac{1}{10}\begin{bmatrix}10\\7-j7\\-10\\7-j7\end{bmatrix},$$

$$\begin{bmatrix}g_0\\g_1\\g_2\\g_3\end{bmatrix}=\frac{1}{10}\begin{bmatrix}10\\7+j7\\-10\\7+j7\end{bmatrix}.$$

取 $\{d'_n\}$ 和 $\{g'_n\}$ 如下：

$$\begin{bmatrix}d'_0\\d'_1\\d'_2\\d'_3\end{bmatrix}=\begin{bmatrix}10\\7-j7\\-10\\7-j7\end{bmatrix},\qquad\begin{bmatrix}g'_0\\g'_1\\g'_2\\g'_3\end{bmatrix}=\begin{bmatrix}10\\7+j7\\-10\\7+j7\end{bmatrix}.$$

先求 $\{d'_n\}$ 与 $\{g'_n\}$ 的循环卷积，除以 100，就得到 $\{d_n\}$ 和 $\{g_n\}$ 的循环卷积 $\{y_k\}$. 为此，根据 **12** 中的(8)式，模 M 必需满足

$$M>2\cdot 10\cdot 10\cdot 4=800,$$

故取 $M=F_4=2^{16}+1$, $N=4$, $\alpha=2^8$. 于是，变换矩阵 T 及逆变换矩阵 T^{-1} 是($N^{-1}=2^{30}$)：

$$T\equiv\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & 2^8 & -1 & -2^8\\ 1 & -1 & 1 & -1\\ 1 & -2^8 & -1 & 2^8\end{bmatrix}\quad(\text{mod}2^{16}+1),$$

$$T^{-1}\equiv2^{30}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -2^8 & -1 & 2^8\\ 1 & -1 & 1 & -1\\ 1 & 2^8 & -1 & -2^8\end{bmatrix}\quad(\text{mod}2^{16}+1).$$

于是

$$\begin{bmatrix}D'_0\\ D'_1\\ D'_2\\ D'_3\end{bmatrix}\equiv T\begin{bmatrix}d'_0\\ d'_1\\ d'_2\\ d'_3\end{bmatrix}\equiv\begin{bmatrix}14-j14\\ 20\\ -14+j14\\ 20\end{bmatrix}\quad(\text{mod}2^{16}+1),$$

$$\begin{bmatrix}G'_0\\ G'_1\\ G'_2\\ G'_3\end{bmatrix}\equiv T\begin{bmatrix}g'_0\\ g'_1\\ g'_2\\ g'_3\end{bmatrix}\equiv\begin{bmatrix}14+j14\\ 20\\ -14-j14\\ 20\end{bmatrix}\quad(\text{mod}2^{16}+1).$$

利用复数数论变换的循环卷积特性，有

$$\begin{bmatrix}Y'_0\\ Y'_1\\ Y'_2\\ Y'_3\end{bmatrix}=\begin{bmatrix}D'_0G'_0\\ D'_1G'_1\\ D'_2G'_2\\ D'_3G'_3\end{bmatrix}\equiv\begin{bmatrix}392\\ 400\\ 392\\ 400\end{bmatrix}\quad(\text{mod}2^{16}+1).$$

取其逆变换，得到

$$\begin{bmatrix} y'_0 \\ y'_1 \\ y'_2 \\ y'_3 \end{bmatrix} \equiv T^{-1} \begin{bmatrix} Y'_0 \\ Y'_1 \\ Y'_2 \\ Y'_3 \end{bmatrix} \equiv \begin{bmatrix} 396 \\ 0 \\ -4 \\ 0 \end{bmatrix} \quad (\mathrm{mod} 2^{16}+1).$$

按模 M 取其绝对最小剩余，得到 $\{d'_n\}$ 和 $\{g'_n\}$ 的循环卷积的真值为

$$\begin{bmatrix} 396 \\ 0 \\ -4 \\ 0 \end{bmatrix}.$$

各项除以 100，得到

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 3.96 \\ 0 \\ -0.04 \\ 0 \end{bmatrix}.$$

各项分别乘以 $(W_4^{\frac{1}{2}})^{k^2}(k=0, 1, 2, 3)$，得到

$$\begin{bmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \end{bmatrix} = \begin{bmatrix} 3.96 \\ 0 \\ -0.04 \\ 0 \end{bmatrix} \approx \begin{bmatrix} 4 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

此即所给 $\{x_n\}$ 的 DFT.

二、计算序列的相关函数

在 **5** 中数论变换的相关特性中已讲到这个问题. 设 $\{x_n\}$ 和 $\{h_n\}(n=0, 1, \cdots, N-1)$ 是以 N 为周期的周期序列，它们的相关函数定义为

$$y_n=\sum_{m=0}^{N-1} x_m h_{n+m} \quad (n=0,\ 1,\ \cdots,\ N-1). \tag{9}$$

如果 $x_n=h_n(n=0,\ 1,\ \cdots,\ N-1)$，就称为自相关函数.

根据数论变换的相关特性，有

$$Y_k \equiv X_{N-k}\cdot H_k (\mathrm{mod} M) \quad (k=0,\ 1,\ \cdots,\ N-1),$$

其中，$\{X_k\}=\mathrm{NTT}\{x_n\}$，$\{H_k\}=\mathrm{NTT}\{h_n\}$，

$$\{Y_k\}=\mathrm{NTT}\{y_n\}.$$

因此，再将 $\{Y_k\}$ 进行反变换就得到 $\{y_n\}$. 所以相关函数的计算按下式进行：

$$\{y_n\}=\mathrm{INTT}\{\mathrm{NTT}\{x_{N-n}\}\cdot\mathrm{NTT}\{h_n\}\}.$$

由上式知，我们可把相关函数的计算变为循环卷积的计算. 事实上，设 $a_n=x_{N-n}$，$b_n=h_n$ $(n=0,\ 1,\ \cdots,\ N-1)$，作 $\{a_n\}$，$\{b_n\}$ 的循环卷积 $\{z_n\}$：

$$z_n=\sum_{k=0}^{N-1} a_k b_{\langle n-k\rangle_N}=\sum_{k=0}^{N-1} x_{N-k} h_{\langle N-k+n\rangle_N}$$

$$=\sum_{m=0}^{N-1} x_m h_{m+n} \quad (n=0,\ 1,\ 2,\ \cdots,\ N-1).$$

故 $$y_n=z_n \quad (n=0,\ 1,\ \cdots,\ N-1).$$

三、计算整多项式的乘法

设 $$f(x)=\sum_{i=0}^{N-1} a_i x^i, \qquad g(x)=\sum_{i=0}^{N-1} b_i x^i$$

为 x 的多项式，其中 a_i，b_i 是复整数*. 它们的乘积是

* 我们这里虽然假设两个多项式的次数相同，但这已包含了次数不相同的情况，因为我们总可补零使次数不相同的多项式变成次数相同的情况. 又若 a_i，b_i 不是复整数，则可将 $f(x)$ 和 $g(x)$ 适当处理，然后再用下法求其乘积.

$$h(x)=f(x)g(x)=\sum_{i=0}^{N-1}\sum_{k=0}^{N-1}a_i b_k x^{i+k}$$

$$=\sum_{m=0}^{2N-2}\Big[\sum_{\substack{n=0\\0\leqslant m-n\leqslant N-1}}^{N-1} a_n b_{m-n}\Big]x^m=\sum_{m=0}^{2N-2}c_m x^m,$$

其中，

$$c_m=\sum_{n=0}^{N-1}a_n b_{m-n}\quad(m=0,\ 1,\ \cdots,\ 2N-2),$$

$$a_n=b_n=0\quad(n<0,\ n\geqslant N).\tag{10}$$

式(10)是一种卷积，但这个卷积与我们在**1**中介绍的卷积略有不同．(10)式中的序列$\{a_n\}$和$\{b_n\}$的长度是N，而要求输出序列$\{c_m\}$的长度是$2N-1$．但不难将(10)式的卷积化为一般的卷积(**1**中的(1)式)．

设
$$\hat{a}_n=\begin{cases}a_n, & n=0,\ 1,\ \cdots,\ N-1,\\ 0, & n=N,\ N+1,\ \cdots,\ 2N-2;\end{cases}$$

$$\hat{b}_n=\begin{cases}b_n, & n=0,\ 1,\ \cdots,\ N-1,\\ 0, & n=N,\ \cdots,\ 2N-2.\end{cases}$$

作$\{\hat{a}_n\}$和$\{\hat{b}_n\}$的卷积，就得(10)式的卷积值：

$$c_m=\sum_{n=0}^{2N-2}\hat{a}_n\hat{b}_{m-n}\quad(m=0,\ 1,\ \cdots,\ 2N-2).\tag{11}$$

(11)式是非循环卷积，如果将它化为循环卷积，则可用数论变换计算．

例 2 设$f(x)=6x^3+3x^2+9x+10$,

$g(x)=2x^3+5x^2+6x+9$，求$h(x)=f(x)g(x)$．

【解】 $N=4,\ 2N-2=6$．

$$\{a_n\}=\begin{bmatrix}10\\9\\3\\6\end{bmatrix},\qquad \{b_n\}=\begin{bmatrix}9\\6\\5\\2\end{bmatrix},$$

$$\{\hat{a}_n\}=\begin{bmatrix}10\\9\\3\\6\\0\\0\\0\end{bmatrix},\qquad \{\hat{b}_n\}=\begin{bmatrix}9\\6\\5\\2\\0\\0\\0\end{bmatrix}.$$

计算 $\{\hat{a}_n\}$ 和 $\{\hat{b}_n\}$ 的卷积 $\{c_m\}$ $(m=0, 1, \cdots, 5)$，有

$$\{c_m\}=\begin{bmatrix}90\\141\\131\\137\\69\\36\\12\end{bmatrix},$$

故

$$h(x)=12x^6+36x^5+69x^4+137x^3+131x^2+141x+90.$$

四、计算两个大整数的乘积

设 A、B 均为整数，将它们表为 u 进位制数(如 $u=10$，则为 10 进制数)：

$$A=\sum_{i=0}^{N-1} a_i u^i,\quad B=\sum_{i=0}^{N-1} b_i u^i,$$

其中，$0\leqslant a_i<u$，$0\leqslant b_i<u$ $(i=0, 1, \cdots, N-1)$. 将它们相乘得

$$C=\sum_{i=0}^{2N-2} l_i u^i, \tag{12}$$

其中，
$$l_m=\sum_{n=0}^{N-1} a_n b_{m-n} \quad (m=0,\ 1,\ \cdots,\ 2N-2),$$
$$a_n=b_n=0 \quad (n<0,\ n\geqslant N). \tag{13}$$
式(13)可与(10)式一样计算，但这样计算出的 l_m 不一定满足 $0\leqslant l_m<u(m=0,\ 1,\ \cdots,\ 2N-2)$，因此还必需把 C 表示成 u 进制数．这个问题不难解决，但因与数论变换无关，故不再细述，读者可参考文献[11]．

为了说明起见，举一例说明．例中的数字不太大，数若很大，算法是一样的．

例 3 设 $A=151,\ B=239$，求 AB 之值．

【解】 将 A 和 B 写作 10 进制数：

$$A=151=1\cdot 10^2+5\cdot 10+1, \quad B=239=2\cdot 10^2+3\cdot 10+9.$$

于是
$$\{a_n\}=\begin{bmatrix}1\\5\\1\end{bmatrix}, \qquad \{b_n\}=\begin{bmatrix}9\\3\\2\end{bmatrix}.$$

根据第三段的方法，作长为 $2N-1$ 的序列

$$\{\hat{a}_n\}=\begin{bmatrix}1\\5\\1\\0\\0\end{bmatrix}, \qquad \{\hat{b}_n\}=\begin{bmatrix}9\\3\\2\\0\\0\end{bmatrix}.$$

计算 $\{\hat{a}_n\}$ 和 $\{\hat{b}_n\}$ 的卷积，这可用数论变换求得为

$$\{l_n\}=\begin{bmatrix}9\\48\\26\\13\\2\end{bmatrix}.$$

故

$$C=151\cdot 239=2\cdot 10^4+13\cdot 10^3+26\cdot 10^2$$
$$+48\cdot 10+9=36089.$$

当 A 和 B 很大时(即 N 很大),利用数论变换计算 $\{\hat{a}_n\}$, $\{\hat{b}_n\}$ 的卷积,其优越性即可显出.

-16-

数论变换用的代码

数论变换和快速傅里叶变换一样，可以在通用计算机上实现，也可以设计专门的硬件．由于数论变换的运算法是以 M 为模的同余运算，它和通常的四则运算有所差别，因此，这些专用的硬件在逻辑结构上有它自己的特点．在设计这些专用的硬件时，首先要按照模运算的特点，找到参加运算的数的合适的代码．在这一节里，着重介绍这些代码的运算法则，并且主要介绍以 Fermat 数 F_t 为模的运算．

一、普通二进制码

使用 FNT 是以模 $F_t=2^b+1(b=2^t)$ 的运算，运算过程中所有的整数按模 F_t 取值．因此，只有 0, 1, 2, …, 2^b 等 2^b+1 个数参加运算，所以寄存器一般需要 $b+1$ 位．如果运算时寄存器是 b 位，那么 0, 1, 2, …, 2^b-1 等所有整数都能表示出来，但是 2^b，也就是 -1 却表示不出．然而，如果上面 2^b+1 个数是互不相关的，那么出现 2^b 的概率是 $1/(2^b+1)$，在数字滤波中，b 一般取作 16、32 或 64，因此出现 2^b 的概率是很小的．倘若出现 2^b(即 -1)，就以 0 或 -2 代替，误差不大．如果不允许这个误差，那么就应当再加一位，成为 $b+1$ 位，但这时最高位是表示 2^b 的，当这位是 1 时，其它各位必需是零，否则将会出现大于 F_t 的数．

下面讨论模 F_t 的各种运算，这些运算是以寄存器只有 b

位来讨论的.

(一)负数的表示法

设正整数 $A=\sum_{i=0}^{b-1}a_i 2^i$, $a_i=0$ 或 1, 又设 a_i 的反码是 $\bar{a}_i$, $a_i+\bar{a}_i=1$, 于是

$$
\begin{aligned}
-A&=-\sum_{i=1}^{b-1}a_i 2^i=\sum_{i=0}^{b-1}(\bar{a}_i-1)2^i\\
&=\sum_{i=1}^{b-1}\bar{a}_i 2^i-(2^b-1)\equiv\sum_{i=0}^{b-1}\bar{a}_i 2^i+2 \pmod{F_t}.
\end{aligned}
$$

这表示, 在二进制寄存器中, 数 A 取负的操作是对原数按位取反码再加 2 即得.

例 1 $F_t=17$, $b=4$, $A=9$, 求 -9.

由于 $$9=1001,$$

$$
-9=\left\{\begin{array}{r}0\ 1\ 1\ 0\\ +0\ 0\ 1\ 0\\ \hline 1\ 0\ 0\ 0\end{array}\right\}=1000=8.
$$

故 $$-9\equiv 8 \pmod{17}.$$

(二)两数相加

两个 b 位数相加, 用通常的二进制加法, 或者仍为 b 位数, 这时不作处理即得结果; 或者溢出 1 位, 这溢出的 1 位表示 $2^b\equiv-1 \pmod{F_t}$. 因此如果出现溢出时, 对相加结果减去 1 即得.

例 2 $F_t=17$, $b=4$, $A=7$, $B=5$, 求 $A+B$.

由于 $7=0111$, $5=0101$, 于是

$$
\begin{array}{r}0\ 1\ 1\ 1\\ +0\ 1\ 0\ 1\\ \hline 1\ 1\ 0\ 0\end{array}=12,
$$

故 $$7+5=12.$$

例 3 $F_t=17$, $b=4$, $A=12$, $B=9$, 求 $A+B$.

由于 $12=1100$, $9=1001$, 于是

$$\begin{array}{r} 1\ 1\ 0\ 0 \\ +1\ 0\ 0\ 1 \\ \hline 1\ 0\ 1\ 0\ 1, \end{array} \qquad \begin{array}{r} 0\ 1\ 0\ 1 \\ -0\ 0\ 0\ 1 \\ \hline 0\ 1\ 0\ 0 \end{array} =4.$$

故 $$12+9\equiv 4 \pmod{17}.$$

(三)两数相减

先将减数取负,然后与被减数相加.

例 4 $F_t=17$, $b=4$, $A=15$, $B=9$, 求 $A-B$.

由于 $15=1111$, $9=1001$, $-9=1000$, 于是

$$\begin{array}{r} 1\ 1\ 1\ 1 \\ +1\ 0\ 0\ 0 \\ \hline 1\ 0\ 1\ 1\ 1, \end{array} \qquad \begin{array}{r} 0\ 1\ 1\ 1 \\ -0\ 0\ 0\ 1 \\ \hline 0\ 1\ 1\ 0 \end{array} =6.$$

故 $$15-9\equiv 15+8\equiv 6 \pmod{17}.$$

(四)两数相乘

A 和 B 都是 b 位数, 其积一般需要 $2b$ 位表示. 设 $C=A\times B$, 我们把 C 分作高 b 位和低 b 位, 分别用 C_H, C_L 表示. 于是

$$C=A\times B=C_L+C_H\cdot 2^b\equiv C_L-C_H \pmod{F_t}.$$

所以,乘积按模 F_t 所取的值是它的低 b 位减去高 b 位所得的值.

例 5 $F_t=17$, $b=4$, $A=13$, $B=9$, 求 $A\times B$.

由于 $13=1101$, $9=1001$

$$
\begin{array}{r}
1101 \\
\times 1001 \\
\hline
1101 \\
1101 \\
\hline
\underbrace{0111}_{C_H}\underbrace{0101}_{C_L},
\end{array}
\qquad
\begin{array}{lr}
C_L & 0101 \\
-C_H & 1010 \\
 + & \\
\hline
 & 1111 = 15.
\end{array}
$$

故 $$13 \times 9 \equiv 15 \pmod{17}.$$

如果 $B = 2^k (0 < k < b)$，对整数 A 乘以 2^k 的操作过程如下：将 A 放入 b 位寄存器中，左移 k 位，移位时的溢出保留在高位寄存器中，作为 C_H，移位完毕仍留在 b 位寄存器中的数就为 C_L，从 C_L 减 C_H 就得结果.

同样，如果 $B = 2^{-k}$，对整数 A 乘以 2^{-k} 时，将 A 放入 b 位寄存器中，右移 k 位，移出的位逐位存入另一 b 位寄存器中，最后从左边寄存器中的余数位减去右边寄存器中的数即得结果. 这是由于

$$
\begin{aligned}
A \cdot 2^{-k} &= (a_{b-1}2^{b-1} + a_{b-2}2^{b-2} + \cdots + a_k 2^k + \cdots + a_0) \cdot 2^{-k} \\
&= a_{b-1}b^{b-1-k} + \cdots + a_k + a_{k-1}2^{-1} + \cdots + a_0 2^{-k} \\
&\equiv (a_{b-1}2^{b-1-k} + \cdots + a_k) \\
&\quad - (a_{k-1}2^{b-1} + \cdots + a_0 2^{b-k}) \pmod{F_t}
\end{aligned}
$$

的缘故.

例 6 $F_t = 17$, $b = 4$, $A = 11$, $B = 2^3$, 求 $A \cdot 2^3$.

由于 $11 = 1011$，将它左移三位得 $\underbrace{0101}_{C_H}\underbrace{1000}_{C_L}$，于是

$$
\begin{array}{lr}
C_L & 1000 \\
-C_H & 1100 \\
 + & \\
\hline
 & 10100,
\end{array}
\qquad
\begin{array}{r}
0100 \\
-0001 \\
\hline
0011 = 3.
\end{array}
$$

故 $$11 \cdot 2^3 \equiv 3 \pmod{17}.$$

例 7 $F_t=17$, $b=4$, $A=11$, $B=2^{-3}$, 求 $A\cdot 2^{-3}$.

由于 $11=1011$, 右移三位得 $\underbrace{0\,0\,0\,1}_{C_H}\,\underbrace{0\,1\,1\,0}_{C_L}$,

于是

$$\begin{array}{lr} C_H & 0\,0\,0\,1 \\ -C_L & 1\,0\,1\,1 \\ \quad + & \\ \hline & 1\,1\,0\,0 \end{array} =12.$$

故 $11\cdot 2^{-3}\equiv 12\pmod{17}$. 这结果是正确的，事实上，$2^{-1}\equiv 9 \pmod{17}$, $11\cdot 2^{-3}\equiv 11\cdot 9^3=8019\equiv 12\pmod{17}$.

以上是用普通二进制码来进行模 F_t 的运算，但有时感到不很方便. 例如在作减法时，我们定义的减法是

$$A-B=A+(-B),$$

取负按上面规定的方法操作. 但是当 $B=1$ 时，却只能用一般的减法而不能用这里规定的操作，否则得不出结果. 这就是说，要根据不同的情况采取不同的操作. 这在乘法时也出现类似的情况. 这种情况之所以发生，主要是用了 b 位寄存器，以至 -1 无法表示. 另外，当 FNT 运算结果出现 -1 时，就会出现整个数据发生错误，虽然这种概率很小，但确实存在.

如果使用下面的两种代码，就不会出现上述情况.

二、新　码

设 $M=F_t=2^b+1$, $b=2^t$. 寄存器用 $b+1$ 位. 新码是定义一个用来表示模 F_t 整数的新二进制码. 设整数 A 的 $b+1$ 位二进制表示为

$$A=[a_b,\ a_{b-1},\ \cdots,\ a_1,\ a_0].$$

规定如下:

(i) 当 $a_b=1$ 时，其它各位必需全为零，表示 $A=0$；

(ii) 当 $a_b=0$ 时，A 的值为

$$A=\sum_{i=0}^{b-1}\sigma_i 2^i, \qquad (*)$$

其中 $$\sigma_i=\begin{cases}1, & a_i=1\\ -1, & a_i=0\end{cases} \quad (i=0,\ 1,\ \cdots,\ b-1).$$

例如，$b=4$ 时，10000 表示 0，01100 表示 $9(1\cdot 2^3+1\cdot 2^2-1\cdot 2-1\cdot 2^0=9)$。也就是说 9 的新码是 01100，5 的新码是 01010。通常这种表示方法只能表示奇数，但是在做模 F_t 运算后，奇数和偶数都能表示了。事实上，(*)的第 j 位所提供的数是

$$(2a_j-1)2^j,\quad a_j=0 \text{ 或 } 1,\ 0\leqslant j\leqslant b-1.$$

故(*)式表示的 A 的数值是

$$\begin{aligned}A&=(2a_{b-1}-1)\cdot 2^{b-1}+(2a_{b-2}-1)\cdot 2^{b-2}+\cdots+(2a_0-1)\\&=a_{b-1}\cdot 2^b+a_{b-2}\cdot 2^{b-1}+\cdots+2a_0-(2^b-1)\\&\equiv(a_{b-2}2^{b-1}+\cdots+2a_0-a_{b-1}+2)\pmod{F_t}.\end{aligned}$$

这个式子表示 $1\sim 2^b$ 的所有数，而零是用 $a_b=1$ 来表示的，这样所有的数都能表示了。

用这种新码可以进行取负，加法，减法以及与 2 的方幂的乘法。读者可参阅文献[12]。

三、亏 一 码

亏一码比新码更为方便[13]。

(一)数码的表示

设 A 为正整数，用 $A-1$ 的二进制码表示 A，就叫 A 的

亏一码. 码长仍为 $b+1$. 如 $b=4$, 5 的亏一码就是 00100. 详见表 10.

表 10 普通二进制码与亏一码之间关系($b=4$)

数　　值	普通二进码	亏一码
1	0 0 0 0 1	0 0 0 0 0
2	0 0 0 1 0	0 0 0 0 1
3	0 0 0 1 1	0 0 0 1 0
4	0 0 1 0 0	0 0 0 1 1
5	0 0 1 0 1	0 0 1 0 0
6	0 0 1 1 0	0 0 1 0 1
7	0 0 1 1 1	0 0 1 1 0
8	0 1 0 0 0	0 0 1 1 1
9(−8)	0 1 0 0 1	0 1 0 0 0
10(−7)	0 1 0 1 0	0 1 0 0 1
11(−6)	0 1 0 1 1	0 1 0 1 0
12(−5)	0 1 1 0 0	0 1 0 1 1
13(−4)	0 1 1 0 1	0 1 1 0 0
14(−3)	0 1 1 1 0	0 1 1 0 1
15(−2)	0 1 1 1 1	0 1 1 1 0
16(−1)	1 0 0 0 0	0 1 1 1 1
0	0 0 0 0 0	1 0 0 0 0

(二)负数的表示

从表 10 可以看出,每一个负数和它对应的正数是互为反码(后 b 位),例如 $-4=01100$, $4=00011$. 事实上,一般地可证明如下:

设 A 的亏一码是 $A-1$, 它的低 b 位的反码记为 $\overline{A-1}$, 则

$$\overline{A-1}=2^b-1-(A-1)=2^b+1-A-1$$
$$\equiv(-A)-1 \quad (\mathrm{mod} F_t).$$

这就表示 A 的亏一码的低 b 位的反码即为 $-A$ 的亏一码. 如

果最高位(第 $b+1$ 位)是1，则不能取负.

例1 $F_t=17$, $b=4$, $A=4$, 求 $-A$.

由于4的亏一码是00011，后四位取反码，则为01100，此为13的亏一码. 故 $-4\equiv 13 \pmod{17}$.

(三)**两数相加**

数 A 和 B 的亏一码各为 $A-1$, $B-1$, 和数 $A+B$ 的亏一码是 $A+B-1$, 它们之间有

$$A+B-1=[(A-1)+(B-1)]+1.$$

这表示两数之和的亏一码等于两数亏一码之和再加1. 这里有两种情况: (i) $(A-1)+(B-1)$ 如无进位，则末位加1即得结果; (ii) $(A-1)+(B-1)$ 如有进位，由于 $2^b\equiv -1 \pmod{F_t}$，因此相加结果应减去1，与加1相抵消，所以相加后 b 位即是结果. 由上可知加法的操作过程是: (i)两数最高位都是零，则相加后，将其最高位的反码加到最低位，最高位本身归零; (ii)两数最高位如有一个是1，禁止相加，另一个就是和.

例2 $F_t=17$, $b=4$. 求 (1) $8+14$; (2) $4+6$; (3) $5+12$.

(1)
```
   0 0 1 1 1          8
  +0 1 1 0 1        +14
  ----------        -----
   1 0 1 0 0        22≡5 (mod 17);
    \
  +  `------→0
  ----------
   0 0 1 0 0 =5,
```

(2)
```
   0 0 0 1 1          4
  +0 0 1 0 1         +6
  ----------        -----
   0 1 0 0 0         10;
    \
  +  `------→1
  ----------
   0 1 0 0 1 =10,
```

$$
\begin{array}{lrl}
(3) & 0\ 0\ 1\ 0\ 0 & \quad 5 \\
 & +0\ 1\ 0\ 1\ 1 & \quad +12 \\
\hline
 & 0\ 1\ 1\ 1\ 1 & \quad 17\equiv 0 \quad (\mathrm{mod}\ 17). \\
 & \searrow \rightarrow 1 & \\
\hline
 & 1\ 0\ 0\ 0\ 0 = 0, &
\end{array}
$$

(四)两数相减

与普通二进制码一样，先将减数取负，然后和被减数相加.

例 3 $F_t=17$, $b=4$, $A=7$, $B=5$, 求 $A-B$.

由于 $7=00110$, $5=00100$, $-5=01011$, 于是

$$
\begin{array}{rr}
0\ 0\ 1\ 1\ 0 & 7 \\
+0\ 1\ 0\ 1\ 1 & -5 \\
\hline
1\ 0\ 0\ 0\ 1 & 2. \\
\searrow \rightarrow 0 & \\
\hline
0\ 0\ 0\ 0\ 1 = 2, &
\end{array}
$$

(五)乘 2 的方幂

先考虑乘 2. $A\times 2$ 应是 $2A$, 其亏一码是 $2A-1$, A 的亏一码是$A-1$, 故有

$$(A-1)\times 2=(2A-1)-1,$$

故
$$(2A-1)=2(A-1)+1.$$

这表示，乘 2, 就将 A 的代码的后 b 位左移一位并加 1 修正. 这时如果进位, 与两数相加一样, 最末位减 1, 与加 1 相抵消; 如果不进位, 末位加 1 即可. 因此乘 2 的操作是: 如果 A 的最高位是 1, 禁止相乘, 结果为零; 如果 A 的最高位是零, 将 A 的亏一码的后 b 位左移一位, 再将最高位的反码加到最低位.

乘 2^k 时(k 为正整数), 将乘 2 的操作重复 k 次.

例 4 $F_t=17$, $b=4$, $A=11$, 求 $11\cdot 2^3$.

由于 $11=01010$, 后四位左移一位得 10100, 最高位是 1, 故将 0 加于最末位，得 00100；这数的后四位再左移一位得 01000，最高位是 0，故将 1 加于最末位得 01001；这数的后四位再左移一位得 10010，最高位是 1，将 0 加于最末位得 00010, 此即 3 的亏一码, 故 $11\cdot 2^3=88\equiv 3 \pmod{17}$. 为清楚起见, 再用竖式计算如下:

$$\begin{array}{rl} 11 & 01010, \\ 2\cdot 11 & 00100=5, \\ 2^2\cdot 11 & 01001=10, \\ 2^3\cdot 11 & 00010=3. \end{array}$$

即 $$8\times 11=2^3\times 11=2\times 2\times 2\times 11=88\equiv 3 \pmod{17}.$$

(六)一般乘法

数 A 的亏一码是 $A-1$, 数 B 的亏一码是 $B-1$, 乘积 AB 的亏一码是 $AB-1$, 将代码 $(A-1)$ 和 $(B-1)$ 相乘, 得

$$\begin{aligned}(A-1)(B-1)&=AB-(A+B)+1\\ &=(AB-1)-(A+B-1)+1,\end{aligned}$$

故 $$AB-1=(A-1)(B-1)+(A+B-1)-1.$$

由此可知, A, B 两数相乘的操作过程是:

(1) 将 A, B 的亏一码 $(A-1)$, $(B-1)$ 的后 b 位按二进制相乘, 得 $2b$ 位数;

(2) 将 A, B 的亏一码按亏一码相加法则相加, 得 $(A+B-1)$ 的亏一码;

(3) 将 $(A-1)(B-1)$ 与 $(A+B-2)$ 按二进制相加;

(4) 将(3)的结果分为高 b 位和低 b 位, 各用 C_H 和 C_L 表示, 结果是 $C_L+C_H2^b\equiv C_L-C_H \pmod{F_t}$, 即 C_L 加上 $(-C_H)$ 的亏一码, 即得结果.

如果两数中有一数的亏一码的最高位(第 $b+1$ 位)是 1,

禁止相乘，结果为零.

例 5 $F_t=17$, $b=4$, $A=15$, $B=10$, 求 AB.

由于 $15=01110$, $10=01001$, 按上述(1)～(4)进行运算:

(1)
$$\begin{array}{r} 1\,1\,1\,0 \\ \times 1\,0\,0\,1 \\ \hline 1\,1\,1\,0 \\ 1\,1\,1\,0\quad\quad\quad \\ \hline 0\,1\,1\,1\,1\,1\,1\,0, \end{array}$$

(2)
$$\begin{array}{r} 0\,1\,1\,1\,0 \\ +0\,1\,0\,0\,1 \\ \hline 1\,0\,1\,1\,1 \\ +\quad\longrightarrow 0 \\ \hline 0\,0\,1\,1\,1, \end{array}$$

(3)
$$\begin{array}{r} 0\,1\,1\,1\,1\,1\,1\,0 \\ +\quad 0\,0\,1\,1\,1 \\ \hline \underbrace{1\,0\,0\,0}_{C_H}\,\underbrace{0\,1\,0\,1}_{C_L}, \end{array}$$

(4)
$$\begin{array}{rr} C_L & 0\,0\,1\,0\,1 \\ -C_H & 0\,0\,1\,1\,1 \\ + & \\ \hline & 0\,1\,1\,0\,0 \\ & +\longrightarrow 1 \\ \hline & 0\,1\,1\,0\,1=14. \end{array}$$

故
$$15\times10\equiv14\pmod{17}.$$

再介绍另一种乘法. 如果 A, B 两数均非零，那么先把它们的亏一码转换为普通二进制码，按二进制码作乘法，得 $2b$ 位，将它分作高 b 位和低 b 位，分别记作 C_H, C_L. 再按亏一码减法作 C_L-C_H, 就得到积的亏一码，从而得到结果.

例 6 $F_t=17$, $b=4$, $A=15$; $B=10$, 求 AB.

由于 15 和 10 的亏一码分别为 01110, 01001, 所以它们的普通二进制分别是 01111, 01010. 作它们的乘法，分出 C_H, C_L, 再按亏一码减法作 C_L-C_H, 就得到:

$$
\begin{array}{r}
01111 \\
\times 01010 \\
\hline
11110 \\
11110 \\
\hline
\underbrace{1001}_{C_H}\underbrace{0110}_{C_L},
\end{array}
$$

$$
\begin{array}{rr}
C_L & 00110 \\
-C_H & 00110 \\
+ & \\
\hline
 & 01100 \\
 & \searrow\!\!\longrightarrow 1 \\
\hline
 & 01101 = 14.
\end{array}
$$

故 $$15 \cdot 10 \equiv 14 \pmod{17}.$$

参 考 文 献

[1] B. Gold, C. M. Rader, A. V. Oppenheim, and T. G. Stockham, "Digital Processing of Signals", Mcgraw-Hill Book Company, Inc., New York, 1969.

[2] R. C. Agarwal and C. S. Burrus, "Number Theoretic Transforms to Implement Fast Digital Convolution", Proc. IEEE 63, 550(1975).

[3] —"Fast Convolution Using Fermat Number Tramsforms With Application to Digital Filtering", IEEE Trans. Acoustics, Speech and Signal Processing ASSP-22, pp. 87～97. Apr. 1974.

[4] —"Fast One-Dimensional Digital Convolution by Multidimensional Techniques", IEEE Trans. Acoustics, Speech and Signal Processing ASSP-22, 1974.

[5] H. J. Nussbaumer, "Complex Convolutions Via Fermat Number Transforms", IBM J. Res. Develop. 20. 282 1976.

[6] —"Digital Filtering Using Pseudo Fermat Number Transforms", IEEE Trans. Acoustics, Speech and Signal Processing, ASSP-25 Feb. 1977.

[7] C, M. Rader, "Discrete Convolutions Via Mersenne Transforms", IEEE Trans. Comput., Vol. C-21. Dec. 1972.

[8] 四川大学，数丁，"数论变换"，《数学的实践与认识》，3,4, 1977.

[9] E. Vegh, and L. M. Leibowitz, "Fast Complex Convolution Using Number Theoretic Tramsforms", Submitted to the IEEE Trans. Acoustics, Speech and Signal Processing, Apr. 1975.

[10] 华罗庚，数论导引，科学出版社，1957.

[11] J. M. Pollard, "The Fast Fourier Transform in a Finite Field", Mathematics of Computation, Apr. 1971. Vol. 25 pp. 365～374.

[12] J. H. McClellan, "Hardware Realization of a Fermat Number Transform", IEEE Trans. Acoustics, Speech and Signal Processing, 24(1976), pp. 216～225.

[13] L. M. Leibowitz, "Simplified Binary Arithmetic for the Fermat Number Transform", IEEE Trans. Vol. ASSP～24, No. 5 Oct. 1976. pp. 356～359.

[14] 蒋增荣，"复数数论变换"，长沙工学院《工学学报》，1978 年第一期。

[General Information]
书名=数论变换
作者=蒋增荣
页数=192
SS号=10236752
DX号=
出版日期=1980年08月第1版
出版社=上海科学技术出版社